ELSEVIER

Annals of Pure and Applied Logic 77 (1996) 1–34

ANNALS OF PURE AND APPLIED LOGIC

Pell equations and exponentiation in fragments of arithmetic

Paola D'Aquino[1]

Dipartimento di Matematica, Università degli Studi, Via del Capitano 15, 53100 Siena, Italy

Received 12 July 1993; revised 17 January 1995; communicated by A. Nerode

Abstract

We study the relative strength of the two axioms
(*P*) Every Pell equation has a nontrivial solution
(*exp*) Exponentiation is total
over weak fragments, and we show they are equivalent over IE_1.

We then define the graph of the exponential function using only existentially bounded quantifiers in the language of arithmetic expanded with the symbol $\#$, where $\#(x, y) = x^{[\log_2 y]}$. We prove the recursion laws of exponentiation in the corresponding fragment.

1. Introduction

Let $\mathscr{L}$ be the first-order language of arithmetic containing the symbols $0, 1, +, \cdot, \leqslant$, and PA the formal system of Peano Arithmetic whose axioms consist of the set P^- of the axioms of discretely ordered semirings together with the axiom scheme of induction. By restricting the induction scheme to various formulas of the arithmetical hierarchy we obtain subsystems of PA which are usually called fragments of PA. We define the formula classes E_n, U_n, Δ_0, $\forall_n$, $\exists_n$, Π_n, Σ_n in the usual way:

$$E_0 = U_0 = \exists_0 = \forall_0 = \{\phi(\bar{x})\colon \phi \text{ is quantifier free}\},$$

$$\exists_{n+1} = \{\exists \bar{y}\phi(\bar{x}, \bar{y})\colon \phi \in \forall_n\},$$

$$\forall_{n+1} = \{\forall \bar{y}\phi(\bar{x}, \bar{y})\colon \phi \in \exists_n\},$$

$$E_{n+1} = \{\exists \bar{y} \leqslant t(\bar{x})\ \phi(\bar{x}, \bar{y})\colon \phi \in U_n, t \text{ a term of } \mathscr{L}\},$$

$$U_{n+1} = \{\forall \bar{y} \leqslant t(\bar{x})\ \phi(\bar{x}, \bar{y})\colon \phi \in E_n, t \text{ a term of } \mathscr{L}\},$$

$$\Delta_0 = \Sigma_0 = \Pi_0 = \bigcup_{n\in\mathbb{N}} E_n = \bigcup_{n\in\mathbb{N}} U_n,$$

[1] This paper has been written when the author was supported by Istituto Nazionale di Alta Matematica.

SSDI 0168-0072(95)00018-6

$$\Sigma_{n+1} = \{\exists \bar{y}\phi(\bar{x}, \bar{y})\colon \phi \in \Pi_n\},$$

$$\Pi_{n+1} = \{\forall \bar{y}\phi(\bar{x}, \bar{y})\colon \phi \in \Sigma_n\}.$$

The symbol $\bar{x}$ denotes a tuple of variables $x_1, \ldots, x_n$. In the formula $\phi(\bar{x}, \bar{y})$ there is no connection between the length of the tuples $\bar{x}$ and $\bar{y}$.

For $\mathscr{C}$ one of Δ_0, U_n, E_n, Π_n, Σ_n, $\forall_n$, $\exists_n$ we will denote by $I\mathscr{C}$ the theory axiomatized by P^- together with the axiom scheme

$$\forall \bar{y}((\phi(0, \bar{y}) \wedge \forall x(\phi(x, \bar{y}) \to \phi(x + 1, \bar{y}))) \to \forall x\phi(x, \bar{y})).$$

as ϕ runs through $\mathscr{C}$.

The theory IE_0 (which is the same as IU_0, $I\exists_0$, $I\forall_0$) will be denoted *IOpen*.

The relative strength of these systems is the following:

$$IOpen \subsetneq IE_1 \subseteq IE_2 \subseteq \cdots \subseteq I\Delta_0 \subsetneq I\Sigma_1 \subsetneq I\Sigma_2 \subsetneq \cdots \subsetneq PA,$$

where the symbol $\subseteq$ denotes that it is still unknown if the inclusion is proper or not. This may be related to the problem of the collapse of the Δ_0-hierarchy (see [15]), but the precise relation is not understood yet.

$\mathbf{N}$ will denote the standard model of $I\mathscr{C}$, and $\mathscr{M}$ will denote both the structure and the domain of any non standard model of $I\mathscr{C}$. We will be mainly concerned with $I\Delta_0$, its fragments and extensions.

The following is due to Parikh [11].

Fact 1.1. *Let* $\theta(x_1, \ldots, x_n, y) \in \Delta_0$ *and assume* $I\Delta_0 \vdash \forall x_1, \ldots, x_n \exists y\theta(x_1, \ldots, x_n, y)$. *Then* $I\Delta_0 \vdash \forall x_1, \ldots, x_n \exists y < (\max(2 + x_i))^k \theta(x_1, \ldots, x_n, y)$ *for some* $k \in \mathbb{N}$.

So any Δ_0-definable function which is provably total in $I\Delta_0$ is bounded by a polynomial.

Paris showed that there is a Δ_0-formula $E_0(x, y, z)$ defining the graph of exponentiation and satisfying the usual recursion laws in $I\Delta_0$ (see [5]):

(1) $\forall x > 0 E_0(x, 0, 1)$,

(2) $\forall x \forall y \forall z(E_0(x, y, z) \to E_0(x, y + 1, xz))$,

(3) $\forall x \forall y \forall z(E_0(x, y + 1, z) \to \exists w < z E_0(x, y, w))$.

The two results imply that exponentiation is not a provably total function in $I\Delta_0$. This is one of the main obstacles in reproducing in $I\Delta_0$ very basic theorems of elementary number theory, such as the cofinality of primes, since we do not have functions of at least exponential growth at hand. Let *exp* be the sentence

$$\forall x \forall y \exists z E_0(x, y, z).$$

The system $I\Delta_0 + exp$ has been widely studied, and it has turned out to be strong enough to reproduce almost all elementary number theory. (In the sequel we will often denote $E_0(x, y, z)$ by the more suggestive notation $x^y = z$.)

Woods studied the scheme Δ_0-PHP below, which is a weak version of the usual pigeon-hole principle. The scheme consists of all instances of the following, as θ ranges through all Δ_0-formulas:

Δ_0-PHP: $\forall \bar{w} \forall z(\forall x < z + 1 \exists y < z \theta(x, y, \bar{w}) \rightarrow \exists x_1, x_2 < z + 1 \exists y < z$

$$(x_1 = x_2 \wedge \theta(x_1, y, \bar{w}) \wedge \theta(x_2, y, \bar{w}))), \quad \text{where } \theta(x, y, \bar{w}) \in \Delta_0.$$

He showed that $I\Delta_0 + \Delta_0$-PHP$\vdash$*cofinality of primes*. This result was then improved by Paris, Wilkie and Woods by showing that only a weak version of the pigeon-hole principle is in fact necessary (see [12]), namely,

Δ_0-WPHP: for all x there is no 1–1 Δ_0-function f such that $f: 2x \rightarrow x$.

The principle Δ_0-WPHP is available in the theory $I\Delta_0 + \Omega_1$, where Ω_1 is

$$\forall x \exists y(x^{\log x} = y),$$

and by $\log x$ we mean the integer part of $\log_2 x$, which has a well-defined meaning. We will use this convention through the paper.

The system $I\Delta_0 + \Omega_1$ has been widely studied. It has emerged as an economical system where an easy coding of syntax is possible (see [16]). Among the extensions of $I\Delta_0$ the following strict relations hold:

$$I\Delta_0 \subset I\Delta_0 + \Omega_1 \subset I\Delta_0 + exp.$$

Fragments such as $I\Delta_0$ and $I\Delta_0 + \Omega_1$ have been shown to have strict connections with complexity theory [15]. Many open problems in such theories have complexity theoretic counterparts. For example, it is still open whether $I\Delta_0$ proves all instances of the MRDP-theorem. By MRDP-theorem we understand (and we will use this standard notation also in the following) the fundamental theorem due to Matijasevic, Robinson, Davis and Putnam, which asserts that every Σ_1-set is purely existentially definable. As observed by Wilkie a positive solution to this problem would solve in a positive way the well-known open problem if NP = co-NP. It is also unknown if the theory $I\Delta_0 + \Omega_1$ proves the MRDP-theorem. A positive answer would also imply NP = co-NP. On the other hand, Gaifman and Dimitracopoulos proved that $I\Delta_0 + exp \vdash$ MRDP-theorem (see [5]).

Motivated by these problems we will study the theory of Pell equations in $I\Delta_0$ (in the classical proof of the MRDP-theorem Pell equations play a fundamental role). We will consider the relative strength of the axiom *exp* and the axiom

(*P*) Every Pell equation has a nontrivial solution

over weak fragments.

We will use then solutions of suitable Pell equations to define the graph of the exponential function using only existentially bounded quantifiers in an expanded language. And we will prove the usual properties of exponentiation using the appropriate induction.

Notation. $x < y$ stands for $x \leqslant y \wedge x \neq y$, $\sqrt{x}$ will denote the unique y satisfying the formula $y^2 \leqslant x < (y+1)^2$, $[x/y]$ will denote the unique z satisfying $zy \leqslant x < (z+1)y$, and $x|y$ stands for $\exists q \leqslant y(y = qx)$.

2. Preliminaries

We begin by recalling a few definitions and properties of models of $I\Delta_0$ and weaker fragments. Let $\mathcal{M} \vDash I\Delta_0$. We will denote by $\mathcal{M}$ both the structure and the domain. We say that an element $p \in \mathcal{M}$ is *irreducible* iff $p > 1 \wedge \forall y \leqslant p(y|p \leftrightarrow y = 1 \vee y = p)$, while we say that p is *prime* iff $p > 1 \wedge \forall y \forall z(p|yz \rightarrow (p|y \vee p|z))$.

Wilmers showed in [17] that the two notions coincide over IE_1. This is a consequence of Bezout's theorem which can be proved in IE_1. So when we work in models of IE_1 or $I\Delta_0$ we will use the Δ_0-definition of prime as an irreducible element. In *IOpen* the notions of *prime* and *irreducible* are distinct.

Lemma 2.1. *Let A be a bounded nonempty Δ_0-definable subset of $\mathcal{M}$. Then A has a maximal element.*

Because of the nontotality of exponentiation it is not always possible to define in a Δ_0-way the notion of *sum of a Δ_0-sequence*. A sufficient condition in order to do it is given in [12], where it is proved that in case we deal with a Δ_0-sequence of "small" length and whose terms are bounded there is a Δ_0-formula defining the graph of the function representing the sum of the sequence.

Theorem 2.2. *Let $a, b, d \in \mathcal{M}$, $d \leqslant (\log a)^k$ for some $k \in \mathbf{N}$ and $F: d \rightarrow b$, Δ_0-definable. Then there is a Δ_0-definable function $G: d \rightarrow \mathcal{M}$ (definable uniformly in terms of any parameters in the definition of F) such that $G(0) = F(0)$ and for all $i < d$, $G(i+1) = G(i) + F(i+1)$, i.e. the sum of the function F* exists.

In [3] a local theory of summations is developed, and the obvious properties of sums are proved under the hypothesis of Theorem 2.2. We will use them tacitly, and we refer to [3] for the details. Theorem 2.2 was also used in [3] to give a Δ_0-meaning to the functions *factorial* and *binomial coefficient*. The recursion properties of these functions were proved in $I\Delta_0$. So in the following we will simply write $n!$ and $\binom{n}{k}$ for the Δ_0-formulas defining them.

Let $d \in \mathcal{M}$. If d is not a square then $\sqrt{d}$ is *irrational* in $\mathcal{M}$, in other words

$$\mathcal{M} \vDash \forall a \leqslant d(a^2 \neq d) \rightarrow \forall x \forall y(x^2 = dy^2 \rightarrow x = 0 \wedge y = 0).$$

Recall that this is not true in every model of *IOpen*. From now on suppose d is not a square. We will work with the quadratic extension $\mathcal{M}[\sqrt{d}]$ whose elements will be

represented by the standard notation $a + \sqrt{d}b$ where $a, b \in \mathcal{M}$. We will refer to a as the rational part of $a + \sqrt{d}b$ and b as the irrational part of $a + \sqrt{d}b$. (Notice that the notation $\sqrt{d}$ we use here is not exactly the same of the Introduction, but we feel sure that no confusion will arise.) In a natural way we can extend the operations of $+$ and $\cdot$ to $\mathcal{M}[\sqrt{d}]$. It is also convenient to define an order on $\mathcal{M}[\sqrt{d}]$, by

$$p + \sqrt{d}q < r + \sqrt{d}s \text{ iff } (p - r)^2 < d(s - p)^2.$$

Next we extend the notion of integer part of $x + \sqrt{d}y \in \mathcal{M}[\sqrt{d}]$:

$[x + \sqrt{d}y] = z$ iff z is the greatest element of $\mathcal{M}$ satisfying $z \leqslant x + \sqrt{d}y$ (or equivalently, $(z - x)^2 \leqslant dy^2$)

This definition makes sense because of Lemma 2.1, where $A = \{w: (w - x)^2 \leqslant dy^2\}$ is clearly Δ_0-definable and bounded by $x + dy$.

It makes sense now to talk about the fractional part of an element of $\mathcal{M}[\sqrt{d}]$. We define $\{x + \sqrt{d}y\} = x + \sqrt{d}y - [x + \sqrt{d}y]$.

We need to prove the following lemma.

Lemma 2.3. *If $t \neq y$ then $\{x + \sqrt{d}y\} \neq \{z + \sqrt{d}t\}$ for all x, z.*

Proof. Let $x, y, z, t \in \mathcal{M}$ and assume $\{x + \sqrt{d}y\} = \{z + \sqrt{d}t\}$. This implies $x + \sqrt{d}y - [x + \sqrt{d}y] = z + \sqrt{d}t - [z + \sqrt{d}t]$, so $x - z + \sqrt{d}(y - t) = [x + \sqrt{d}y] - [z + \sqrt{d}t]$. Hence $y - t = 0$, which is a contradiction. □

Norm: In a very natural way we can define the norm of an element $x + \sqrt{d}y$ of $\mathcal{M}[\sqrt{d}]$ by $N(x + \sqrt{d}y) = x^2 - dy^2$.

Exponentials: Next we define the nth power of an element $x + y\sqrt{d}$ of $\mathcal{M}[\sqrt{d}]$. Recall the standard definition

(●) $(x + y\sqrt{d})^n = \sum_{i \leqslant n} \binom{n}{i} x^{n-i} y^i d^{i/2}$.

So we get an element of the quadratic extension whose rational and irrational parts x_n and y_n are given by

$$x_n = \sum_{\substack{i \leqslant n \\ i \equiv 0(2)}} \binom{n}{i} x^{n-i} y^i d^{i/2}$$

and

$$y_n = \sum_{\substack{i \leqslant n \\ i \equiv 1(2)}} \binom{n}{i} x^{n-i} y^i d^{(i-1)/2},$$

respectively.

We will formalize this definition in such a way that the relation $(x + y\sqrt{d})^n = u + v\sqrt{d}$ will be defined using only bounded quantifiers. The main ingredients are the Δ_0-definitions of the exponential function and of the binomial coefficient. Hence both the functions $F_1, F_2 : [0, n] \to \mathscr{M}$

$$F_1(i) = \begin{cases} \binom{n}{k} x^{n-i} y^i d^{i/2} & \text{if } i \equiv 0 (\text{mod } 2), \\ 0 & \text{if } i \equiv 1 (\text{mod } 2), \end{cases}$$

$$F_2(i) = \begin{cases} \binom{n}{i} x^{n-i} y^i d^{(i-1)/2} & \text{if } i \equiv 1 (\text{mod } 2), \\ 0 & \text{if } i \equiv 0 (\text{mod } 2) \end{cases}$$

are Δ_0-definable.

Notice that the values of F_1 and F_2 are bounded by u and v, respectively, and from $(x + \sqrt{d}y)^n = u + \sqrt{d}v$ it follows that n is a logarithm. So by Theorem 2.2 the sums of the functions F_1 and F_2 both exist; denote them by G_1 and G_2. So we define

$$(*) \qquad (x + y\sqrt{d})^n = u + v\sqrt{d} \text{ iff } G_1(n) = u \wedge G_2(n) = v.$$

In the above definition we have been a bit imprecise, what we really mean by writing $G_1(n) = u$ and $G_2(n) = v$ are the Δ_0-formulas which define the functions G_i's.

Let $\mathscr{R}_{\mathscr{M}}$ denote the ring associated to $\mathscr{M}$. It is possible to extend the above notions also to $\mathscr{R}_{\mathscr{M}}[\sqrt{d}]$, but it involves more technical complications. For our purposes we only need the notions of sum, product, and norm of elements of $\mathscr{R}_{\mathscr{M}}[\sqrt{d}]$, but these can be easily defined from the corresponding definitions in $\mathscr{M}[\sqrt{d}]$.

From the definition of power of an element of $\mathscr{M}[\sqrt{d}]$ it is clear that it is only a partial function. The next lemma gives necessary and sufficient conditions for the existence of the nth power of an element of $\mathscr{M}[\sqrt{d}]$.

Lemma 2.4. *Let $x, y, u, v, n \in \mathscr{M}$. The following are equivalent:*

(i) *there exist u, v satisfying $u + v\sqrt{d} = (x + y\sqrt{d})^n$;*

(ii) *there exist $a, b, c \in \mathscr{M}$ such that $a = x^n$, $b = y^n$, $c = d^n$.*

Proof. (i) $\Rightarrow$ (ii) This follows directly from the definition of power.

(ii) $\Rightarrow$ (i) If all the three objects x^n, y^n, d^n exist, then the functions

$$F_1(i) = \begin{cases} \binom{n}{k} x^{n-i} y^i d^{i/2} & \text{if } i \equiv 0 (\text{mod } 2), \\ 0 & \text{otherwise}, \end{cases}$$

$$F_2(i) = \begin{cases} \binom{n}{i} x^{n-i} y^i d^{(i-1)/2} & \text{if } i \equiv 1 (\text{mod } 2), \\ 0 & \text{otherwise} \end{cases}$$

are defined for all $i \leqslant n$. The domains of definition have logarithmic length and the values of both are bounded in $\mathscr{M}$, say by $(4xyd)^n$. Hence by Theorem 2.2 the functions F_1, F_2 admit sums G_1, G_2, and $G_1(n) + G_2(n) = (x + y\sqrt{d})^n$. □

But for those elements for which the power is defined we will prove that the basic properties are satisfied.

Lemma 2.5.

(1) $(x + y\sqrt{d})^n = u + v\sqrt{d} \to (x + y\sqrt{d})^{n+1} = ux + dyv + (xv + yu)\sqrt{d}$;

(2) $(x + y\sqrt{d})^{n+1} = w + t\sqrt{d} \to \exists u < w \exists v < t((x + y\sqrt{d})^n = u + v\sqrt{d} \wedge w = ux + dyv \wedge t = xv + yu)$;

(3) $(x + y\sqrt{d})^{n+m} = (x + y\sqrt{d})^n (x + y\sqrt{d})^m$;

(4) $((x + y\sqrt{d})^n)^m = (x + y\sqrt{d})^{nm}$;

(5) $((x + y\sqrt{dT10})(z + t\sqrt{d}))^n = (x + y\sqrt{d})^n (z + t\sqrt{d})^n$.

Proof. We just sketch the proof; we will use some properties about "infinite" sums and binomial coefficient which were proved in [3], without mentioning them everytime.

(1) Assume n is odd. First of all notice that the sums of the functions F_1, F_2: $[0, n+1] \to \mathcal{M}$ defined as

$$F_1(i) = \begin{cases} \binom{n+1}{i} x^{n+1-i} y^i d^{i/2} & \text{if } i \equiv 0 (\text{mod } 2), \\ 0 & \text{otherwise,} \end{cases}$$

$$F_2(i) = \begin{cases} \binom{n+1}{i} x^{n+1-i} y^i d^{i-1/2} & \text{if } i \equiv 1 (\text{mod} 2), \\ 0 & \text{otherwise} \end{cases}$$

do exist since the domains of definition are of logarithmic length and the values of F_1 and F_2 are clearly bounded. We want to show that $\sum_{i \leqslant n} F_1(i) = ux + dyv$ and $\sum_{i \leqslant n} F_2(i) = uy + vx$. From the hypothesis it follows that

$$ux + dyv = \left(\sum_{\substack{i=0 \\ i \equiv 0(2)}}^{n} \binom{n}{i} x^{n-i} y^i d^{i/2} \right) x + \left(\sum_{\substack{i=0 \\ i \equiv 1(2)}}^{n} \binom{n}{i} x^{n-i} y^i d^{(i-1)/2} \right) yd$$

$$= \sum_{\substack{i=0 \\ i \equiv 0(2)}}^{n} \binom{n}{i} x^{n+1-i} y^i d^{i/2} + \sum_{\substack{i=0 \\ i \equiv 1(2)}}^{n} \binom{n}{i} x^{n-i} y^{i+1} d^{(i+1)/2} = \binom{n}{0} x^{n+1}$$

$$+ \sum_{\substack{i=1 \\ i \equiv 0(2)}}^{n} x^{n+1-i} y^i d^{i/2} + \sum_{\substack{i=0 \\ i \equiv 1(2)}}^{n-1} \binom{n}{i} x^{n-i} y^{i+1} d^{(i+1)/2} + \binom{n}{n} y^{n+1} d^{(n+1)/2}.$$

But

$$\sum_{\substack{i=0 \\ i \equiv 1(2)}}^{n-1} \binom{n}{i} x^{n-i} y^{i+1} d^{(i+1)/2} + \sum_{\substack{i=0 \\ i \equiv 0(2)}}^{n} \binom{n}{i-1} x^{n+1-i} y^i d^{i/2},$$

so

$$
\begin{aligned}
&ux + dyv \\
&= \binom{n+1}{0} x^{n+1} + \sum_{\substack{i=1 \\ i \equiv 1(2)}}^{n} \sum_{\substack{i=1 \\ i \equiv 0(2)}}^{n} \left(\binom{n}{i} + \binom{n}{i-1} \right) x^{n+1-i} y^i d^{i/2} \\
&\quad + \binom{n+1}{n+1} y^{n+1} d^{(n+1)/2} \\
&= \binom{n+1}{0} x^{n+1} + \sum_{\substack{i=1 \\ i \equiv 0(2)}}^{n} \binom{n+1}{i} x^{n+1-i} y^i d^{i/2} + \binom{n+1}{n+1} y^{n+1} d^{(n+1)/2} \\
&= \sum_{\substack{i \leqslant n+1 \\ i \equiv 0(2)}} \binom{n+1}{i} x^{n+1-i} y^i d^{i/2}.
\end{aligned}
$$

Consider now the second coordinates, from the hypothesis it follows that

$$
\begin{aligned}
uy + vx &= \left(\sum_{\substack{i=0 \\ i \equiv 0(2)}}^{n} \binom{n}{i} x^{n-i} y^i d^{i/2} \right) y + \left(\sum_{\substack{i=0 \\ i \equiv 1(2)}}^{n} \binom{n}{i} x^{n-i} y^i d^{(i-1)/2} \right) x \\
&= \sum_{\substack{i=0 \\ i \equiv 0(2)}}^{n} \binom{n}{i} x^{n-i} y^{i+1} d^{i/2} + \sum_{\substack{i=0 \\ i \equiv 1(2)}}^{n} \binom{n}{i} x^{n+1-i} y^i d^{(i-1)/2} \\
&= \sum_{\substack{i=1 \\ i \equiv 1(2)}}^{n+1} x^{n+1-i} y^i d^{(i-1)/2} + \sum_{\substack{i=0 \\ i \equiv 1(2)}}^{n} \binom{n}{i} x^{n+1-i} y^i d^{(i-1)/2} \\
&= \sum_{\substack{i=0 \\ i \equiv 1(2)}}^{n+1} \binom{n}{i-1} x^{n+1-i} y^i d^{(i-1)/2} + \sum_{\substack{i=0 \\ i \equiv 1(2)}}^{n+1} \binom{n}{i} x^{n+1-i} y^i d^{(d-1)/2} \\
&= \sum_{\substack{i=0 \\ i \equiv 1(2)}}^{n+1} \left(\binom{n}{i-1} + \binom{n}{i} \right) x^{n+1-i} y^i d^{(i-1)/2} = \sum_{\substack{i=0 \\ i \equiv 1(2)}}^{n+1} \binom{n+1}{i} x^{n+1-i} y^i d^{(i-1)/2}.
\end{aligned}
$$

Notice that in the last two equalities we have used the fact that n is odd and so components congruent to 0 modulo 2 do not give any contribution to the sums.

In case n is even analogous arguments are used.

(2) From the definition of power in $\mathscr{M}[\sqrt{d}]$, if $(x + y\sqrt{d})^{n+1} = w + t\sqrt{d}$ it means that the sums of the functions F_1, F_2 defined as in (1), both exist. Consider the functions $f_1, f_2 : [0, n] \to \mathscr{M}$ defined as

$$
f_1(i) = \begin{cases} \binom{n}{k} x^{n-i} y^i d^{i/2} & \text{if } i \equiv 0 (\text{mod } 2), \\ 0 & \text{otherwise,} \end{cases}
$$

$$f_2(i) = \begin{cases} \binom{n}{i} x^{n-i} y^i d^{(i-1)/2} & \text{if } i \equiv 1 (\text{mod } 2), \\ 0 & \text{otherwise.} \end{cases}$$

It is clear that $f_j(i) \leqslant F_j(i)$ for all $i \leqslant n$ and $j = 1, 2$. So the sums of the functions f_1, f_2 exist, say g_1, g_2, respectively, and $g_1(n) \leqslant G_1(n+1) = w$ and $g_2(n) \leqslant G_2(n+1) = t$. Now just repeat the same proof as in (1).

The proofs of (3), (4) are very similar, in both cases fix $x, y, n, u, v \in \mathcal{M}$ such that $(x + \sqrt{d}y)^n = u + \sqrt{d}v$ and apply induction on m. The proof of (5) uses a slightly more complex inductive argument. Fix $x, y, n, u, v, a, b \in \mathcal{M}$ such that

$$((x + \sqrt{d}y)\,(u + \sqrt{d}v))^n = a + \sqrt{d}b.$$

We want to show that there are c, h, e, k such that $(x + \sqrt{d}y)^n = c + \sqrt{d}h$, $(u + \sqrt{d}v)^n = e + \sqrt{d}k$ and $ce + dhk = a$ and $eh + kc = b$. This is proved by induction on $i \leqslant n$. We omit the tedious proof. □

It will be useful to extend also the notion of negative power in a restricted context.

Definition 2.6. Let $x, y, n \in \mathcal{M}$, and $x^2 - dy^2 = 1$. Define

$$(x + y\sqrt{d})^{-1} = x + (-y)\sqrt{d}, \quad \text{and} \quad (x + y\sqrt{d})^{-n} = ((x + y\sqrt{d})^n)^{-1}.$$

Note that $(x + \sqrt{d}y)^{-1} \in \mathcal{R}_M[\sqrt{d}]$, and $(x + \sqrt{y})\,(x + \sqrt{d}y)^{-1} = 1$.

Notation. Let $x + \sqrt{d}y \in \mathcal{M}$. We will denote the coordinates of the nth power of $x + \sqrt{d}y$ by (x_n, y_n), while $(x + \sqrt{d}y)^{-n}$ has coordinates (x_{-n}, y_{-n}). From the above definition it follows $(x_{-n}, y_{-n}) = (x_n, -y_n)$.

3. The local theory of Pell equations

We recall that a Pell equation is of the form

(*) $\quad X^2 - dY^2 = 1,$

where d is not a square. The notation $d \neq \square$ will be used as an abbreviation of $\forall a \leqslant d(a^2 \neq d)$. It is a well known theorem of $\mathbb{N}$ that any Pell equation has a non trivial solution, i.e. a solution other than $x = \pm 1$, $y = 0$. Let (P) denote the property

(P) Any Pell equation has a nontrivial solution.

We want to analyze the proof of this statement over weak fragments of PA and to understand the "strength" of it. In $\mathbb{N}$ a proof of (P) follows immediately from the proof

that the quadratic extension $\mathbb{Q}(\sqrt{d})$ has nontrivial units. We will follow the proof which uses Dirichlet theorem on diophantine approximations, which is proved by a pigeon-hole argument (see [1]). In fact we need only a weak version of the pigeon-hole principle. This will enable us to prove the following version of Dirichlet theorem in $I\Delta_0 + \Omega_1$. Note that Baker's proof [1] of the existence of a non-trivial solution of a Pell equation needs only the version below of Dirichlet theorem together with an inductive argument which can definitely not be done in $I\Delta_0 + \Omega_1$.

Theorem 3.1. *Let $\mathcal{M} \models I\Delta_0 + \Omega_1$, $d \in \mathcal{M}$, d not a square, $Q > 1$, then there are $p, q \in \mathcal{M}$ such that $|p - \sqrt{d}q| < 1/Q$, and $q < 2Q$.*

Proof. Axiom Ω_1 implies Δ_0-WPHP, i.e. $\mathcal{M} \models \neg\exists 1\text{-}1\Delta_0 f\colon [0, 2a] \to [0, a]$ for all $a \in \mathcal{M}$. Let $h\colon [0, 2Q] \to [0, 1]$ be defined by $h(n) = \{n\sqrt{d}\}$. h is Δ_0-definable, and by Lemma 2.3 it is injective. Let g be a partition of the interval $[0, 1]$ into Q equal parts, i.e. $g\colon [0, Q] \to [0, 1]$, defined as $g(i) = i/Q$. Clearly g is Δ_0-definable, since $g(i) = y$ iff $yQ = i$.

By Δ_0-WPHP we cannot fit the elements of $[0, 2Q]$ into the Q boxes in which $[0, 1]$ has been divided by g. So there must exist $n, k \leqslant 2Q$ with $k < n$ such that $|\{n\sqrt{d}\} - \{k\sqrt{d}\}| < 1/Q$. But $|\{n\sqrt{d}\} - \{k\sqrt{d}\}| = |n\sqrt{d} - [n\sqrt{d}] - k\sqrt{d} + [k\sqrt{d}]|$, so if $p = [n\sqrt{d}] - [k\sqrt{d}]$ and $q = k - n$, it follows that $|p - q\sqrt{d}| < 1/Q$ and $q < 2Q$. □

Clearly, p, q can be chosen coprime. Notice that we can also bound the size of p, since $|p| = |p - \sqrt{d}q + \sqrt{d}q| \leqslant |p - q\sqrt{d}| + q\sqrt{d} < 1/Q + 2Q\sqrt{d} \leqslant 3Q\sqrt{d}$. So what the theorem shows is

$$I\Delta_0 + \Omega_1 \vdash \forall d \forall Q (d \neq \square \to \exists p \leqslant 3Q\sqrt{d} \exists q \leqslant 2Q |p - q\sqrt{d}| < 1/Q).$$

With simple algebraic calculations we can show that the element $\alpha = p - q\sqrt{d}$ of $\mathcal{M}[\sqrt{d}]$ has norm $N(\alpha)$, bounded independently of the choice of Q:

$$|N(p - q\sqrt{d})| = |p - q\sqrt{d}\,|\,|p + q\sqrt{d}| \leqslant |p - q\sqrt{d}|(|p - q\sqrt{d}| + 2q\sqrt{d}|)$$

$$< 1/Q(1/Q + 4Q\sqrt{d}) \leqslant 1/Q 5Q\sqrt{d} = 5\sqrt{d}.$$

The proof of (P) in $\mathbb{N}$ procedes now with an iteration of Dirichlet theorem in order to get infinitely many different pairs (p, q) such that $N(p - q\sqrt{d}) < 5\sqrt{d}$. To be more precise let (p, q) be the pair of integers associated to a starting Q, choosing now $Q_1 > 1/(|p - q\sqrt{d}|)$ we get (p_1, q_1) satisfying $|p_1 - q_1\sqrt{d}| < 1/Q_1$ and moreover $p/q \neq p_1/q_1$. The last inequality is true because of the irrationality of $\sqrt{d}$. Since the norms of all elements $p + \sqrt{d}q$ are bounded by $5\sqrt{d}$, by a pigeon-hole argument there

are infinitely many pairs (p, q) such that $N(p + q\sqrt{d}) = N$, for some $N < 5\sqrt{d}$. Among these there will be at least two pairs (p, q) and (p_1, q_1) such that $p \equiv p_1 (\mathrm{mod}\, N)$ and $q \equiv q_1 (\mathrm{mod}\, N)$. A linear combination of p, p_1, q, q_1, N gives a nontrivial solution of $X^2 - dY^2 = 1$ (see [1]).

It is not in fact necessary to have infinitely many pairs (p, q) constructed as above. With a right use of the pigeon-hole principle we could obtain the same result using only finitely many pairs. We want to estimate how many. If n is the number of pairs we need and whose norm take values $< k = [6\sqrt{d}]$, to be safe, then n/k have the same norm. Among these we want that at least two pairs have congruent coordinates modulo N, for some $N < k$, i.e. we want

$$\frac{n/k}{k^2} > 1,$$

so $n > k^3 = 216d\sqrt{d}$. Applying Dirichlet theorem $432d\sqrt{d}$ times and then the Δ_0-WPHP we get the right number of pairs we need. It is clear that in this procedure a recursive argument is hidden which we need to code in $I\Delta_0 + \Omega_1$ if we want to reproduce the proof of (P) in such a fragment. But Ω_1 does not offer any guarantee that this coding is possible. On the other hand, if exponentiation is total then the coding is possible and we can reproduce the proof of (P), as Dimitracopoulos showed in [4].

Remark 1. We want to give a rough estimate on the size of Q we need to reach in order to get the sufficient number of pairs (p, q) in order to carry on the argument sketched before. Starting with $Q > 1$ which has associated the pair (p, q), a lower bound for Q_1 is

$$\frac{1}{|p - q\sqrt{d}|}.$$

But

$$\frac{1}{|p - q\sqrt{d}|} \leqslant |p + q\sqrt{d}| < 5Q\sqrt{d},$$

so if we choose $Q_1 > 5Q\sqrt{d}$ the pair associated to Q_1 is different from the pair determined by Q. In general, at stage $i + 1$ it is enough to choose $Q_{i+1} > 5Q_i\sqrt{d}$. So if $n = 432d\sqrt{d}$ is the number of pairs (p, q) we need, then the final Q is of the order $(5\sqrt{d})^{432d\sqrt{d}}Q$. These are not the best estimates, but they clearly show that elements of exponential size are involved. Already without coding we need a double exponential.

By simple calculations we get a rough estimate of the amount of exponentiation we need in order to code the whole procedure. Assume we code via the product of powers of primes, so we need at least $432d\sqrt{d}$ primes and the size of the $432d\sqrt{d}$th prime is of the order $432d\sqrt{d} \cdot \log(432d\sqrt{d}) < (432d\sqrt{d})^2 = 432^2d^3$.

Each pair p_i, q_i is coded by an element $\leqslant (12(5\sqrt{d})^i\sqrt{d})^2 = 144 \cdot 5^{2i}d^{i+1}$. So if α is the code of the whole procedure we have

$$\alpha < \prod_{i \leqslant 432^2 d^3} p_i^{144 \cdot 5^{2 \cdot 432 d\sqrt{d}} d^{216 d\sqrt{d}+1}} < 2^{2^{2^{2^4}}}.$$

This estimate gives also an upper bound on the size of the nontrivial solution.

Remark 2. For some Pell equations there is no problem in bounding a nontrivial solution. For example, the equation $X^2 - (a^2 - 1)Y^2 = 1$, where $a \geqslant 2$ is satisfied by the pair $(a, 1)$.

We recall that in $\mathbb{N}$ all the solutions of a Pell equation

$$(\star) \qquad X^2 - dY^2 = 1$$

are generated by the fundamental solution (x_1, y_1) in the sense specified in the following proposition. By (x_1, y_1) minimal we will mean that x_1 (and equivalently, y_1) is smaller than all x (and equivalently, all y) such that $x^2 - dy^2 = 1$.

Proposition 3.2. *Let (x_1, y_1) be a solution of $(\star)$ with x_1, y_1 minimal. Then (x, y) is a solution of $(\star)$ iff $x + y\sqrt{d} = (x_1 + y_1\sqrt{d})^n$ for some $n \in \mathbb{N}$.*

The power $(x_1 + y_1\sqrt{d})^n$ is as specified in Section 2. In this way the set of solutions of the equation $(\star)$ has a semigroup structure. If we consider also negative powers of (x_1, y_1) (see Definition 2.6), then the set of solutions of $(\star)$ have a group structure.

Notation. We will write $(x_n(d), y_n(d))$ to denote the nth solution of the equation $(\star)$. We will also use $(x_n(a), y_n(a))$ to denote the nth solution of the equation $X^2 - (a^2 - 1)Y^2 = 1$. If there is no ambiguity we will simply write (x_n, y_n) for the nth solution.

We want now to extend the notion of nth solution of the equation $(\star)$ to any model of $I\Delta_0$ in such a way that the structure of semigroup is preserved and also some of the basic properties are provable in $I\Delta_0$.

Assume that $(\star)$ has a nontrivial solution, without loss of generality we can assume it is the fundamental solution (x_1, y_1). In Section 2 we defined the power of an element of $\mathcal{M}[\sqrt{d}]$, so we will use that notion. In the following sections we will define the notion of nth solution in a different way using other relations whose ideas were suggested by Robinson–Matijasevic work.

Definition 3.3.

$$u = x_n \text{ iff } u = \sum_{\substack{i \leqslant 0 \\ i \equiv 0(2)}}^{n} \binom{n}{i} x_1^{n-i} y_1^i d^{i/2}$$

and

$$v = y_n \text{ iff } v = \sum_{\substack{i \leqslant 0 \\ i \equiv 1(2)}}^{n} \binom{n}{i} x_1^{n-i} y_1^i d^{(i-1)/2}.$$

As already remarked there are severe restrictions on the existence of the nth solution in a model $\mathcal{M}$ of $I\Delta_0$ since exponentials are involved. But for those which exist we will show that they have the same structure as in the standard case.

Notice that with only algebraic tools we can easily prove that if (u, v) and (w, t) are solution of $(\star)$ then the product of them (as an element of $\mathcal{M}[\sqrt{d}]$) is also a solution, i.e. $(u + \sqrt{d}v)\,(w + \sqrt{d}t) = uw + dvt + \sqrt{d}(ut + vw)$ and $(uw + dvt)^2 - d(ut + vw)^2 = 1$. In the next lemmas we prove that Definition 2.6 gives in fact a solution of $(\star)$ and that any solution of $(\star)$ is a power of the fundamental one. Fix $\mathcal{M} \models I\Delta_0$.

Lemma 3.4. $\mathcal{M} \models \forall n \forall u \forall v (u + v\sqrt{d} = (x_1 + y_1\sqrt{d})^n \to u^2 - dv^2 = 1)$.

Proof. Fix $n, u, v \in \mathcal{M}$ such that $u + v\sqrt{d} = (x_1 + y_1\sqrt{d})^n$. Consider $\theta(k) \stackrel{\text{def}}{=} \exists w \leqslant u\, \exists t \leqslant v (w + \sqrt{d}t = (x_1 + y_1\sqrt{d})^k \wedge w^2 - dt^2 = 1)$. We show that $I\Delta_0 \vdash \forall k \leqslant n \theta(k)$.

$k = 0$: Take $w = 1$ and $t = 0$.

$k \to k + 1 \leqslant n$: By hypothesis there are r, s such that $(x_1 + y_1\sqrt{d})^k = r + s\sqrt{d}$ and $r^2 - ds^2 = 1$. By Lemma 2.5 (1), $(x_1 + y_1\sqrt{d})^{k+1} = rx_1 + dsy_1 + (x_1 s + y_1 r)\sqrt{d}$, and $(rx_1 + dsy_1, x_1 s + y_1 r)$ is a solution of $(\star)$ since product of two solutions. This concludes the proof. □

For future proofs it is useful to show that also negative powers of the fundamental solution are solution of the equation.

Lemma 3.5. *For any $n \in \mathcal{M}$, if $(x_1 + y_1\sqrt{d})^{-n}$ is defined then $(x_1 + y_1\sqrt{d})^{-n}$ is a solution of $(\star)$.*

Proof. The proof proceeds exactly in the same way as in previous lemma and using Definition 2.6. □

Lemma 3.6. $\mathcal{M} \models \forall u \forall v (u^2 - dv^2 = 1 \to \exists n \leqslant u (x_1 + y_1\sqrt{d})^n = u + v\sqrt{d})$.

Proof. Consider the set

$$A = \{m \in \mathcal{M}: \exists w \leqslant u \exists z \leqslant v (w + \sqrt{d}z = (x_1 + \sqrt{d}y_1)^m \wedge w + \sqrt{d}z \leqslant u + \sqrt{d}v)\}.$$

A is Δ_0-definable and it is bounded, hence it has a maximal element n. So $(x_1 + y_1\sqrt{d})^n \leqslant u + v\sqrt{d} < (x_1 + y_1\sqrt{d})^{n+1}$. Multiply the three solutions by $(x_1 + y_1\sqrt{d})^{-n}$, we get again three solutions satisfying $1 \leqslant (u + v\sqrt{d})(x_1 + y_1\sqrt{d})^{-n} < x_1 + y_1\sqrt{d}$. This contradicts the minimality of (x_1, y_1), unless $u + v\sqrt{d} = (x_1 + y_1\sqrt{d})^n$. □

An immediate corollary is

Corollary 3.7. *There is no solution* (u, v) of $(\star)$ *satisfying* $(x_1 + y_1\sqrt{d})^n < u + v\sqrt{d} < (x_1 + y_1\sqrt{d})^{n+1}$.

Remark 3. (i) From previous lemmas we can deduce that for fixed d the functions which associate $n \mapsto x_n(d)$ and $n \mapsto y_n(d)$ are both increasing, i.e. $x_{n+1}(d) \geqslant x_n(d)$ and $y_{n+1}(d) \geqslant y_n(d)$.

(ii) Notice that if (x, y) is a solution of $(\star)$ then x, y are coprime.

Notation. It is useful to recall the properties expressed in Lemma 2.5 from a notat tional point of view, so we are free to use them in what follows. Assume we work with the equation $X^2 - dY^2 = 1$.

(1) $x_{n+m} + \sqrt{d}y_{n+m} = (x_1 + \sqrt{d}y_1)^{n+m} = (x_1 + \sqrt{d}y_1)^n(x_1 + \sqrt{d}y_1)^m = (x_n + \sqrt{d}y_n)(x_m + \sqrt{d}y_m) = x_nx_m + dy_ny_m + \sqrt{d}(x_ny_m + x_my_n)$, i.e. $x_{n+m} = x_nx_m + dy_ny_m$ and $y_{n+m} = x_ny_m + x_my_n$.

(2) $(x_n)_m + \sqrt{d}(y_n)_m = (x_n + \sqrt{d}y_n)^m = ((x_1 + \sqrt{d}y_1)^n)^m = (x_1 + \sqrt{d}y_1)^{nm} = x_{nm} + \sqrt{d}y_{nm}$.

(3) $(x_1 + \sqrt{d}y_1)^n/(x_1 + \sqrt{d}y_1)^m = (x_1 + \sqrt{d}y_1)^n(x_1 + \sqrt{d}y_1) - m = (x_1 + \sqrt{d}y_1)^{n-m} = x_{n-m} + \sqrt{d}y_{n-m}$, and $(x_1 + \sqrt{d}y_1)^n(x_1 + \sqrt{d}y_1)^{-m} = (x_n + \sqrt{d}y_n)(x_m - \sqrt{d}y_m)$, so $x_{n-m} = x_nx_m - dy_ny_m$ and $y_{n-m} = x_my_n - x_ny_m$.

4. Axiom (*P*) over $I\Delta_0$ and IE_1

In this section we will study the *strength* of the axiom

$$(P) \qquad \forall d(d \neq \square \rightarrow \exists x \exists y(x > 1 \wedge x^2 - dy^2 = 1)$$

over the fragments $I\Delta_0$ and IE_1. Note (P) is $\forall\exists$. Our interest was stimulated by results due to Dimitracopoulos and Kaye [4, 8].

First of all, we need to prove some useful facts about solutions of the Pell equation

$$(\star\star) \qquad X^2 - (a^2 - 1)Y^2 = 1, \text{ where } a > 1$$

in $I\Delta_0$. These properties were first discovered by Matijasevic (see an account of it in [10]) in order to give an existential definition of the relation $y = y_n(a)$. He needs in fact additional properties on the set of solutions of $(\star\star)$. We do not recall these since they will not be used in what follows.

Remark 4. From Lemma 2.4 it is clear that $x_n(a)$ and $y_n(a)$ are defined iff a^n is defined, and $x_n(a)$, $y_n(a)$, a^n have all the same rate of growth.

From now on we work in $\mathcal{M} \models I\Delta_0$, and let $a \in \mathcal{M}$, $a > 1$.

Lemma 4.1. *In $\mathcal{M}$ the following are true*:

(1) $\forall n \forall x \forall y (x = x_n \wedge y = y_n \to \sqrt{a^2 - 1}y \leqslant x \leqslant ay)$.
(2) $\forall n \forall y (y = y_{n+1} \to \exists z \leqslant y^2 \exists w \leqslant y (z = (2a)^n \wedge w = (2a-1)^n \wedge w \leqslant y \leqslant z))$
(3) $\forall n \forall x (x = x_n \to x \equiv 1 (\mathrm{mod}\ a-1))$.
(4) $\forall n \forall y (y = y_n \to y \equiv n (\mathrm{mod}\ a-1))$.
(5) $\forall n \forall y (y = y_n \to y \geqslant n)$.
(6) $\forall n \forall m \forall y \forall z (y = y_n \wedge z = y_m \wedge y | z \to n | m)$.
(7) $\forall n \forall m \forall y \forall z (y = y_n \wedge z = y_m \wedge y^2 | z \to y | m)$.

Proof. (1) For fixed $n \in \mathcal{M}$, if $x, y \in \mathcal{M}$ satisfy $x^2 - (a^2-1)y^2 = 1$ then clearly $x^2 > (a^2-1)y^2$, which implies $x > \sqrt{a^2-1}y$; and also $x^2 \leqslant y^2 + (a^2-1)y^2 = (ay)^2$, so $x \leqslant ay$.

(2) Fix $n, y \in \mathcal{M}$ such that $y = y_{n+1}$. Consider the formula
$\theta(k, n, y) \overset{\text{def}}{=} \exists z \leqslant y \exists u \leqslant y \exists v \leqslant y^2 (z = y_k \wedge u = (2a-1)^{k-1} \wedge v = (2a)^{k-1} \wedge u \leqslant z \leqslant v)$.
We want to show $\mathcal{M} \models \forall k \leqslant n (k \geqslant 1 \to \theta(k, n, y))$. Proceed by induction on k.

$k = 1$: Take $z = u = v = 1$.

$k \to k+1 \leqslant n$: Recall that $x_1 = a$ and $y_1 = 1$. By hypothesis there are x_k and y_k. Let $z = ay_k + x_k = y_{k+1}$; because of $k+1 \leqslant n$ and (i) of Remark 3, $z \leqslant y$. There are also elements satisfying $(2a-1)^k, (2a)^k$, and $(2a-1)^k \leqslant (2a-1)^n \leqslant y$, and $(2a)^k \leqslant (2a)^n \leqslant y^2$. By (1), $y_{k+1} = ay_k + x_k \leqslant ay_k + ay_k = 2ay_k \leqslant 2a(2a)^{k-1} = (2a)^k$ and $y_{k+1} \geqslant ay_k + \sqrt{a^2-1}y_k = (a + \sqrt{a^2-1})y_k \geqslant (a + \sqrt{a^2-1})(2a-1)^{k-1} \geqslant (2a-1)(2a-1)^{k-1} = (2a-1)^k$ where the last inequality is true for $a > 1$. This ends the proof.

(3) Fix $n, x \in \mathcal{M}$ such that $x = x_n$, and consider the formula
$\theta(k, n, x) \overset{\text{def}}{=} \exists w \leqslant x (w = x_k \wedge w \equiv 1 (\mathrm{mod}\ a-1))$. We want to show $\mathcal{M} \models \forall k \leqslant n \theta(k, n, x)$. By induction on k.

$k = 0$: Take $w = 1$, clearly $w \equiv 1 (\mathrm{mod}\ a-1)$.

$k \to k+1 \leqslant n$: By hypothesis there are x_k, y_k, so let $w = x_{k+1} = ax_k + (a^2-1)y_k \equiv ax_k (\mathrm{mod}\ a-1) \equiv 1 (\mathrm{mod}\ a-1)$. Also, $x_{k+1} \leqslant x = x_n$.

(4) Fix $n, y \in \mathcal{M}$ such that $y = y_n$, and consider this time the formula
$\theta(k, n, y) \overset{\text{def}}{=} \exists z \leqslant y (z = y_k \wedge z \equiv k (\mathrm{mod}\ a-1))$ and show $\mathcal{M} \models \forall k \leqslant n \theta(k, n, y)$ by induction on $k \leqslant n$.

$k = 0$: Take $z = 0$.

$k \to k + 1 \leqslant n$: Let $z = y_{k+1} = ay_k + x_k \equiv k + 1 (\mathrm{mod}\, a - 1)$, by (3).

(5) This is also proved using the same arguments as before, so we skip the proof of it.

(6) Fix $n, m, y, z \in \mathscr{M}$ such that $y = y_n$, $z = y_m$, $y|z$, and let $\theta(k, n, m, y, z) \overset{\text{def}}{=} \exists v \leqslant z (v = y_k \wedge y|v \to n|k)$. If we show $\mathscr{M} \vDash \forall k \leqslant m \theta(k, n, m, y, z)$, then we have finished. First of all notice that if $y_n|y_m$ then necessarily $n \leqslant m$ (see Remark 3(i)). The inductive argument is slightly different from the other proofs. Fix $k \leqslant m$ and assume that for all $u < k$, $\mathscr{M} \vDash \theta(u, n, m, y, z)$. We want to show that for all $u \leqslant k$ this holds. The only case to prove is for $u = k$. That there is $v = y_k \leqslant z$ is clear, so assume $y_n|y_k$. Recall that $y_{k-n} = x_n y_k - x_k y_n$, hence $y_n|y_{k-n}$ and $k - n < k$, so by inductive hypothesis $n|(k - n)$, so $n|k$.

(7) Let $n, m, y, z \in \mathscr{M}$ such that $y = y_n$, $z = y_m$, and $y^2|z$. > From (6) it follows that $n|m$, so $m = nk$ for some k. Keeping in mind the notation introduced at the end of last section, it is clear that

$$y_m = \sum_{\substack{i \leqslant k \\ i \equiv 1(2)}} x_n^{k-i} y_n^i (a^2 - 1)^{(i-1)/2} \equiv k x_n^{k-1} y_n (\mathrm{mod}\, y_n^2),$$

so $y_n^2 | k x_n^{k-1} y_n$, which implies $y_n | k x_n^{k-1}$. But x_n and y_n are coprime, so necessarily $y_n|k$, hence $y_n|m$. □

Remark 5. We proved (6) and (7) for equations of the type $X^2 - (a^2 - 1) Y^2 = 1$, but in fact they are true for any Pell equation.

We now have all the ingredients to prove

Theorem 4.2. $I\Delta_0 + P \vdash exp$.

Proof. Let $\mathscr{M} \vDash I\Delta_0 + P$. We want to show that exponentiation is a total function on $\mathscr{M}$, i.e. for any $a, c \in \mathscr{M}$ there is an element b in $\mathscr{M}$ satisfying $b = a^c$. Recall that for a fixed basis the logarithmic function is total in $I\Delta_0$. So there is $n \in \mathscr{M}$ such that $a^n \leqslant c < a^{n+1}$. Consider now the Pell equation

(†) $\quad X^2 - (a^2 - 1) Y^2 = 1.$

By Remark 4, the existence of a^{n+1} implies that there is $y \in \mathscr{M}$ satisfying $y = y_{n+1}(a)$; let $x = x_{n+1}(a)$. Now consider the following Pell equation:

(‡) $\quad X^2 - (a^2 - 1)(2x^2y^2)^2 Y^2 = 1.$

From $\mathscr{M} \vDash P$ it follows that (‡) has a nontrivial solution in $\mathscr{M}$, i.e. there are $u, v \in \mathscr{M}$ satisfying $u^2 - (a^2 - 1)(2x^2y^2)^2 v^2 = 1$, and $v > 0$. Let $w = u$ and $z = 2x^2y^2v$. We can show that (w, z) is a solution of (†), i.e. $w^2 - (a^2 - 1) z^2 = u^2 - (a^2 - 1)(2x^2y^2)^2 v^2 = 1$, where last equality is true since (u, v) is a solution of (‡) . By Lemma 3.6, $(u, v) = (x_k(a), y_k(a))$ for some $k \in \mathscr{M}$. Notice that the solutions $y_{n+1}(a)$ and $y_k(a)$ satisfy

$y_{n+1}^2(a)|y_k(a)$, hence by (7) of Lemma 4.1 $y_{n+1}(a)|k$. The existence of the kth solution of (†) implies that a^k is defined in $\mathcal{M}$, and from $y_{n+1}(a) \leqslant k$ it follows that $a^{y_{n+1}(a)}$ has also to be defined. But $y_{n+1}(a) \geqslant a^{n+1}$, which implies $a^{a^{n+1}}$ is defined. Since $c < a^{n+1}$ we can finally deduce that a^c is defined. □

Remark 6. Dimitracopoulos proved in [4] that $I\Delta_0 + exp \vdash P$. So combining his result and Theorem 4.2 we get that the axioms *exp* and (*P*) are equivalent over $I\Delta_0$. This does not support the idea of Jones and Matijasevic in [7] that the axiom (*P*) is weaker than *exp*.

We now want to understand the *strength* of axiom (*P*) over the fragment IE_1. This will be done using some results of Kaye [8]. He proved that if we add the following property:

$$(E) \qquad \forall a \geqslant 2 \forall b \leqslant a - 2 \exists u \exists v (u^2 + v^2 - 2auv - 1 = 0 \wedge u \leqslant v \wedge u \equiv b (\mathrm{mod}\, a - 1) \wedge y \equiv b + 1 (\mathrm{mod}\, a - 1)),$$

to IE_1 then we obtain a system equivalent to $I\Delta_0 + exp$.

First of all notice that, for convenience, he works with equations of the kind $X^2 + Y^2 - 2aXY - 1 = 0$. One of the useful properties that the solutions of these equations satisfy is that if the coordinates of a solution are permuted then we get again a solution, i.e. if (u, v) is a solution, then also (v, u) is a solution. There is a strict relation between equations

$$(\clubsuit) \quad X^2 + Y^2 - 2aXY - 1 = 0 \quad \text{and} \quad (\clubsuit\,\clubsuit) \quad X^2 - (a^2 - 1)Y^2 = 1$$

in the following sense: given any solution (w, z) of $(\clubsuit\,\clubsuit)$ we can construct a solution of $(\clubsuit)$, and vice versa. Let (w, z) satisfy $w^2 - (a^2 - 1)z^2 = 1$, and let $u = w + az$, $v = z$. With easy calculations, (u, v) satisfies $(\clubsuit)$. For the converse, starting from (u, v) satisfying $(\clubsuit)$ construct a solution (w, z) of $(\clubsuit\,\clubsuit)$ by letting $w = u - av$ and $z = v$.

As we saw we can bound all the quantifiers involved in the 'standard' definition of the relation $y = y_n(d)$ in such a way that the notion of nth solution of the equation $X^2 - dY^2 = 1$ is faithfully represented in any model of $I\Delta_0$. It does not seem possible to express this notion in the language $\mathcal{L}$ using only existentially bounded quantifiers. We will discuss this problem in the next sections. It is not even possible to bound the existential quantifiers in the definition of nth solution given by Matijasevic since functions of double exponential growth are used. A congruence relation is on the contrary easily definable by an E_1-formula. So in axiom (*E*) property (4) of Lemma 4.1 is used. In (*E*) the existence of a solution in each class modulo $a - 1$ is required; the one corresponding to class $a - 2$ will be "big", in the sense that it is at least of the order a^{a-2}. So axiom (*E*) says, roughly speaking, that a^a has to be defined.

Kaye's result is

Theorem 4.3 (Kaye [8]). $IE_1 + E \vdash I\Delta_0 + exp$.

On one side, it is quite remarkable that the E_1-induction alone has the power of Δ_0-induction. On the other side, from what we remarked, it is not so surprising that axiom (E) implies that exponentiation is total.

Our original aim was to understand the strength of axiom (P) over IE_1. Using Kaye's result we will prove

Theorem 4.4. $IE_1 + P \vdash I\Delta_0 + exp$.

Before giving the proof of it we notice that axiom (P) has a much simpler formulation than axiom (E). It is a more general statement about Pell equation than (E) is, and does not explicitely require the existence of elements of exponential size.

For the proof we need to recall the following lemma of [8]

Lemma 4.5. $IE_1 \vdash \forall a \geqslant 2 \forall n \leqslant a - 2 \forall x \forall y (x^2 - (a^2 - 1)y^2 = 1 \wedge y \equiv n (\mathrm{mod}\, a - 1) \rightarrow \forall b \leqslant a \forall k \leqslant \min(n, b - 2)\ \exists u < x \exists v < y (u^2 - (b^2 - 1)v^2 = 1) \wedge v \equiv k (\mathrm{mod}\, b - 1))$.

We have stated Lemma 4.5 for the equations $X^2 - (a^2 - 1)\ Y^2 = 1$, where in the original version it was proved for equations of the form $X^2 + Y^2 - 2aXY - 1 = 0$. But as we saw the two formulations are equivalent.

In (3) of Lemma 4.1 we proved in $I\Delta_0$ that the first coordinate of a solution is always congruent to 1 modulo $a - 1$. In the proof of Theorem 4.4 we will use this fact, but we need to prove it using only E_1-induction.

Lemma 4.6. *Let* $\mathcal{M} \models IE_1$ *and* $a, x, y \in \mathcal{M}$, $a > 1$ *satisfy* $x^2 - (a^2 - 1)y^2 = 1$. *Then* $x \equiv 1 (\mathrm{mod}\, a - 1)$

Proof. Consider the formula

$$\theta(t) \overset{\mathrm{def}}{=} \neg \exists x, y \leqslant t (x^2 - (a^2 - 1)\ y^2 = 1 \wedge \neg x \equiv 1 (\mathrm{mod}\, a - 1)).$$

We need to prove that $\mathcal{M} \models \forall t \theta(t)$. Notice that $\theta(t)$ is U_1, but $IE_1 \nvdash IU_1$, so we can apply U_1-induction on $\theta(t)$.

$t = 0$: Immediate.

$t \rightarrow t + 1$: Assume that there are $x, y \leqslant t + 1$ satisfying the equation, but $x \not\equiv 1 (\mathrm{mod}\, a - 1)$. Consider $(x, y)\ (a, 1)^{-1} = (ax - (a^2 - 1)\ y, ay - x) = (w, z)$, clearly $w, z \leqslant t$, and $w \equiv x (\mathrm{mod}\, a - 1)$. So $w \not\equiv 1 (\mathrm{mod}\, a - 1)$, which is a contradiction. □

Proof of Theorem 4.4. We will show that $IE_1 + P \vdash E$. Let $\mathcal{M} \models IE_1 + P$, and $1 < a \in \mathcal{M}$. It is enough to show that there are $x, y \in \mathcal{M}$ such that $x^2 - (a^2 - 1)y^2 = 1$ and $y \equiv a - 2 (\mathrm{mod}\, a - 1)$, since then Lemma 4.5 implies that for all $k \leqslant a - 2$ there is a solution (u, v) such that $v \equiv k (\mathrm{mod}\, a - 1)$, and so $\mathcal{M} \models E$.

Consider the Pell equation $X^2 - (a^2 - 1)(a - 1)^2 Y^2 = 1$. Since $\mathcal{M} \models P$ there are w, z satisfying $w^2 - (a^2 - 1)\ (a - 1)^2 z^2 = 1$. Let $x' = w$ and $y' = z(a - 1)$. It is easy to

check that (x', y') is a solution of $X^2 - (a^2 - 1)Y^2 = 1$, and moreover $y' \equiv 0 (\mathrm{mod}\, a - 1)$, and $y' > 0$. Let now $x = x'a - y'(a^2 - 1)$ and $y = y'a - x'$; using just algebraic calculations it is easy to check that x, y satisfy $x^2 - (a^2 - 1)y^2 = 1$, and using Lemma 4.6, $y \equiv 0 - 1 (\mathrm{mod}\, a - 1) \equiv -1 (\mathrm{mod}\, a - 1) \equiv a - 2 (\mathrm{mod}\, a - 1)$. □

Kaye gets an even stronger result by proving an analogous result of Theorem 4.3 for the theory IE_1^-, where the induction is applied only to existentially bounded formulas with no parameters.

For the sake of completeness we prove an analogous result for axiom (P).

Theorem 4.7. $IE_1^- + P \vdash I\Delta_0 + exp$.

The proof follows the lines of the proof of Corollary 5.9 of [8], so we will not give every single detail.

First of all we need an analogue of Parikh's result for $IE_1 + P$.

Lemma 4.8. *If* $\theta(\bar{x}, \bar{y}) \in \Delta_0$ *and* $IE_1 + P \vdash \forall \bar{x} \exists \bar{y} \theta(\bar{x}, \bar{y})$ *then there is an* $n \in \mathbb{N}$ *such that*

$$IE_1 \vdash \forall \bar{x} \forall z_0, \ldots, z_n \forall u_1, \ldots, u_n \forall v_0, \ldots, v_n (z_0 = \max x_i \wedge$$
$$\bigwedge_{i=0}^{i=n-1} (u_{i+1}^2 - (z_i^2 - 1)(z_i - 1)^2 v_{i+1}^2 = 1$$
$$\wedge u_{i+1} > 1) \wedge z_{i+1} = u_i(z_i - 1) \rightarrow \exists \bar{y} \leqslant z_n \theta(\bar{x}, \bar{y})).$$

Proof. By contradiction. Assume $IE_1 \vdash \forall \bar{x} \exists \bar{y} \theta(\bar{x}, \bar{y})$, but for all $n \in \mathbb{N}$ there is a model $\mathcal{M}_n \models IE_1$ such that $\mathcal{M}_n$ contains $\bar{a}, b_0, \ldots, b_n, c_1, \ldots, c_n, d_1, \ldots, d_n$ satisfying $b_0 = \max a_j$, and for all $i < n$, $c_{i+1}^2 - (b_i^2 - 1)(b_i - 1)^2 d_{i+1}^2 = 1$, and $b_{i+1} = d_{i+1}(b_i - 1)$, and $\mathcal{M}_n \models \forall \bar{y} \leqslant b_n \neg \theta(\bar{a}, \bar{y})$. By compactness there is a model $\mathcal{M}$ of IE_1 containing $\bar{a}, b_0, b_1, \ldots, c_1, c_2, \ldots, d_1, d_2, \ldots$ such that $b_0 = \max a_i$, $c_{n+1}^2 - (b_n^2 - 1)(b_n - 1)^2 d_{n+1}^2 = 1$ and $b_{n+1} = d_{n+1}(b_n - 1)$ for all $n \in \mathbb{N}$, and $\mathcal{M} \models \forall \bar{y} \leqslant b_n \neg \theta(\bar{a}, \bar{y})$ for all $n \in \mathbb{N}$. Let I be the initial segment of $\mathcal{M}$ generated by the b_ns, i.e.

$$I = \{x \in \mathcal{M} : x < b_n \text{ for some } n \in \mathbb{N}\}.$$

Clearly, I is closed under $+, \cdot$, so $I \models IE_1$. Let $e \in I$, so $e < b_n$ for some $n \in \mathbb{N}$. By Lemma 4.5, from $c_{n+1}^2 - (b_n^2 - 1)(b_n - 1)^2 d_{n+1}^2 = 1$ it follows that there are u, v satisfying $u^2 - (e^2 - 1)(e - 1)^2 v^2 = 1$. So $y = v(e - 1)$ is a solution of $X^2 - (e^2 - 1)Y^2 = 1$, $y > 0$ and $y \equiv 0 (\mathrm{mod}\, e - 1)$, and this implies that $I \models E$. So by Theorems 4.3 and 4.4, $I \models IE_1 + P$. But clearly, $\bar{a} \in I$ and $\mathcal{M} \models \forall \bar{y} \leqslant b_n \neg \theta(\bar{a}, \bar{y})$, so $I \models \forall \bar{y} \leqslant b_n \neg \theta(\bar{a}, \bar{y})$ for all $n \in \mathbb{N}$. But this is in contradiction with $IE_1 + P \vdash \forall \bar{x} \exists \bar{y} \theta(\bar{x}, \bar{y})$. □

Lemma 4.8 says that if $IE_1 + P$ proves the totality of a Δ_0-definable function then the values of the function must be bounded by *standard* powers of exponentiation.

We need to recall that IE_1 is a conservative extension of IE_1^- over $\exists\forall E_1$-sentences.

Theorem 4.9 (Kaye [8]). *If σ is a $\exists\forall E_1$-sentence and $IE_1 \vdash \sigma$, then $IE_1^- \vdash \sigma$.*

Corollary 4.10. $IE_1^- + P \vdash I\Delta_0 + exp$.

Proof. Recall that $I\Delta_0 + exp$ has an $\forall\exists$-axiomatization. Let $\sigma = \forall\bar{x}\exists\bar{y}\theta(\bar{x}, \bar{y})$ be an axiom of $I\Delta_0 + exp$. By Theorem 4.4, $IE_1 + P \vdash \sigma$, and by Lemma 4.8 there is $n \in \mathbb{N}$ such that

$$IE_1 \vdash \forall\bar{x}\forall z_0, \ldots, z_n \forall u_1, \ldots, u_n \forall v_1, \ldots, v_n (z_0 = \max x_j \wedge$$
$$\bigwedge_{i=0}^{i=n-1}(u_{i+1}^2 - (z_i^2 - 1)(z_i - 1)^2 v_{i+1}^2 = 1 \wedge z_{i+1} = v_{i+1}(z_i - 1)) \rightarrow \exists\bar{y} \leqslant z_n \theta(\bar{x}, \bar{y})).$$

By Theorem 4.9, IE_1^- proves the previous sentence, and this implies $IE_1^- + P \vdash \sigma$. □

5. $E_1^\#$-definitions of exponentiation

In this section we will define exponentiation in a suitable language using only existentially bounded quantifiers.

J. Robinson was the first to link the theory of Pell equations to definability problems. Her ideas were developed by Matijasevic and their work led to an existential definition of the exponential function, which is one of the main steps in the proof that every r.e. set is existentially definable. Their definition is given in terms of solutions of Pell equations. On the other hand, we know that there is a Δ_0-definition of exponentiation. In this section we are interested in a common refinement of the two definitions from the point of view of complexity of defining formula, i.e. we will try to define the relation $a^n = m$ using only existentially bounded quantifiers. We will only partially succeed. We will first work in $\mathbb{N}$, and then extend the results to fragments of PA.

We recall the existential definition of Robinson and Matijasevic as presented in Manin's book [10].

$$a^n = m \text{ iff } m = [y_{n+1}(Na)/y_{n+1}(N)] \quad \text{for } N > 4nm,$$

where $y_{n+1}(Na)$ is the $(n+1)$st solution of the equation $X^2 - (N^2a^2 - 1)Y^2 = 1$ and $y_{n+1}(N)$ is the $(n+1)$st solution of the equation $X^2 - (N^2 - 1)Y^2 = 1$.

Actually, the argument carried on in Manin's proof does not give a^n as the integer part of $y_{n+1}(Na)/y_{n+1}(N)$, as he claims. This was pointed out to me by Adamovic. What he proves is only that a^n is the nearest integer to $y_{n+1}(Na)/y_{n+1}(N)$. What Manin claims is in fact true, but a different argument is needed for the proof.

Remark 7. It is also possible to define the relation $a^n = m$ using both the rational and irrational parts of the solutions of the two Pell equations: Let

$$z_n(Na) = x_n(Na) + \sqrt{N^2a^2 - 1}y_n(Na) = (Na + \sqrt{N^2a^2 - 1})^n,$$

$$z_n(N) = x_n(N) + \sqrt{N^2 - 1}y_n(N) = (N + \sqrt{N^2 - 1})^n.$$

By an easy induction on n we can prove that $a^n \leqslant z_n(Na)/z_n(N)$; moreover, for fixed n the sequence $z_n(Na)/z_n(N)$ is a decreasing sequence as a function of N. Hence for N large enough $z_n(Na)/z_n(N) < a^n + 1$. So $a^n = [z_n(Na)/z_n(N)]$.

An attempt to modify Paris' definition of exponentiation is not sensible, since that definition involves the notion of prime, and it is not known if we can express such a notion in an E_1-way.

So we will work with the Robinson–Matijasevic definition. Obviously, such a definition presupposes an existential definition of the nth solution of the Pell equation $X^2 - (a^2 - 1)Y^2 = 1$. The relation $y = y_n(a)$ has been uniformly defined for all $a, n, m \in \mathbb{N}$ by Matijasevic using some number theoretic properties of the solutions of a Pell equation which involve functions of double exponential growth. There is no hope of bounding the quantifiers over elements of double exponential size. But for our purposes we do not need a uniform definition of the nth solution. The relation on a, n, y

$$\exists x(x^2 - (a^2 - 1)y^2 = 1 \wedge y \equiv n(\mathrm{mod}\, a - 1))$$

is E_1-definable, but it does not give y as a function of n, a.

The following picture, which is easily constructed using the structure of the congruence relations modulo $a - 1$ of the set of solutions, should clarify the situation:

$$\begin{array}{ccccc}
0 & 1 & 2 & \cdots & a-2 \\
\vdots & \vdots & \vdots & & \vdots \\
y_{-(a-1)} & y_{-(a-2)} & y_{-(a-3)} & \cdots & y_{-1} \\
y_0 & y_1 & y_2 & \cdots & y_{a-2} \\
y_{a-1} & y_a & y_{a+1} & \cdots & y_{2a-3} \\
y_{2a-2} & y_{2a-1} & y_{2a} & \cdots & y_{3a-4} \\
\vdots & \vdots & \vdots & & \vdots
\end{array}$$

Recall that nth solution is roughly speaking of the order a^n. The idea is now to bound the size of the solution in order to pick the smallest positive solution in class n. To do this we need to expand the language of arithmetic with a new functional symbol $\#$ (read sharp), where $\#$ has to be interpreted as $\#(x, y) = x^{\lceil \log_2 y \rceil}$ for all $y > 0$ and $\#(x, 0) = 1$. Denote the expanded language by $\mathscr{L}^{\#}$. The *sharp* function is very closed related to the *smash* function $\sharp$ of Buss, where $\sharp(x, y) = 2^{|x||y|}$ and $|x|$ denotes the length of x in the binary expansion of x (see [2]). Buss works in a language containing also a symbol $|\cdot|$ for the length function. Later we will define a good notion of length in the language $\mathscr{L}^{\#}$ using only existentially bounded quantifiers.

Notice that in the literature the symbol $\#$ has always denoted the function *smash*. Through all the rest of the paper we take the liberty of using $\#$ to denote the *sharp* function, hoping that no confusion will arise. Our choice of the sharp function instead of the smash function has been done only for convenience: calculations seem smoother. We can easily define one function in terms of the other, and vice versa

$$\sharp(x, y) = z \text{ iff } \exists w < z(\#(2, x) = w \wedge \#(w, y) = z)$$

and

$$\#(x, y) = z \text{ iff } z = \text{remainder of the division of } \sharp(\sharp(x, 2y), y) \text{ by } \sharp(x, y) - x.$$

We will first work in $\mathbb{N}$, and then we will consider the two theories in $\mathscr{L}^{\#}$, $I\Delta_0^{\#}$ and $IE_1^{\#}$.

The theory $I\Delta_0^{\#}$ is axiomatized by some basic algebraic axioms concerning $+, \cdot, \leqslant$, the induction scheme restricted to formulas with all quantifiers bounded by terms which may contain $\#$, and the following axioms concerning $\#$:

(1) $\forall x > 0 \forall y(\#(x, 0) = \#(x, 1) = 1 \wedge \#(0, y) = 0)$;

(2) $\forall x > 0 \forall y((Pow_2(y + 1) \wedge \#(x, y + 1) = x\#(x, y)) \vee (\neg Pow_2(y + 1) \wedge \#(x, y + 1) = \#(x, y)))$,

where $Pow_2(x)$ stands for $\forall y \leqslant x(y|x \to 2|y)$, i.e. x is a power of 2.

We will discuss the theory $IE_1^{\#}$ in the next section.

It is easy to check that the theory $I\Delta_0^{\#}$ is biinterpretable with $I\Delta_0 + \Omega_1$ in the following sense:

First of all, $I\Delta_0^{\#} \vdash (\forall x \forall y \forall t \forall z(t = [\log_2 y] \wedge E_0(x, t, z))$. It follows that in any model $\mathscr{M}$ of $I\Delta_0^{\#}$ the function $f(x) = x^{[\log_2 x]}$ is total.

Conversely, if $\mathscr{M} \models I\Delta_0 + \Omega_1$ then the function defined by

$$\theta(x, y, z) = (y = 0 \wedge z = 1) \vee \exists t < y(t = [\log_2 y] \wedge E_0(x, t, z))$$

is provably total in $I\Delta_0 + \Omega_1$, and satisfies the above axioms for $\#$.

Remark 8. (i) Obviously $\#$ does not imply that exponentiation is a total function in $I\Delta_0^{\#}$. But in any model of $I\Delta_0 + \Omega_1$ if 2^n is defined then also 2^{n^k} is defined for all $k \in \mathbb{N}$. Notice also that the domain of definition of exponentiation coincides in this case with the domain of definition of factorial, because of the following inequalities $n! \leqslant n^n \leqslant 2^{n^k}$.

(ii) From a computational point of view $\#$ is less complex than exponentiation, since $\#$ is polynomial time computable, while exponentiation is clearly not.

(iii) The theory $I\Delta_0^{\#}$ (or equivalently, $I\Delta_0 + \Omega_1$) has been considered also as a system where a convenient coding of syntax is feasible (see [16]).

We now go back to our original problem of defining $a^n = m$ using only existentially bounded quantifiers. From now on we work with the language $\mathscr{L}^{\#}$ unless otherwise specified. The next claim gives a bound on the size of the solutions of the Pell equation involved in the Robinson–Matijasevic definition.

Claim. *Let* $m = a^n$, *and* $N = 2nm^2$. *The formula*

$$\theta(a, y, n, m) \stackrel{\text{def}}{=} \exists x \leqslant ay(x^2 - (N^2a^2 - 1)y^2 = 1 \wedge y \equiv n + 1 (\text{mod } Na - 1)$$
$$\wedge 0 < y < (\#(m, m))^6$$

uniquely identifies the smallest positive solution in class $n + 1$.

Proof. Recall that $(2Na - 1)^n \leqslant y_{n+1}(Na) \leqslant (2Na)^n$, and $(2Na)^n \leqslant (2 \cdot 2na^{2n}a)^n \leqslant m \cdot m \cdot m^n \cdot m^{2n} \cdot m \leqslant m^3 \cdot m^{3n} \leqslant m^{6n} \leqslant (\#(m, m))^6$.

On the other hand, the next solution in class $n + 1$ is $y_{n+Na}(Na)$ (see scheme above) and $y_{n+Na}(Na) \geqslant (2Na - 1)^{n+Na-1} \gg m^{m^2} > (m^{log m})^6 = (\#(m, m))^6$. □

Notice that the same bound $(\#(m, m))^6$ also uniquely identifies the smallest positive solution in class $n + 1$ for the equation $X^2 - (N^2 - 1)Y^2 = 1$.

In conclusion, if $\Gamma(a, n, m)$ is

$$\exists y_1 < (\#(m, m))^6 \exists x_1 < m^5 (\#(m, m))^6 \exists y_2 < (\#(m, m))^6 \exists x_2 < m^4 (\#(m, m))^6$$
$$(N = 2nm^2 \wedge x_1^2 - (N^2a^2 - 1)y_1^2 = 1 \wedge x_2^2 - (N^2 - 1)y_2^2 = 1$$
$$\wedge y_1 \equiv n + 1 (\text{mod } Na - 1) \wedge y_2 \equiv n + 1 (\text{mod } N - 1) \wedge m = [y_1/y_2]),$$

then

$$a^n = m \text{ iff } \Gamma(a, n, m).$$

Until now we have worked in the model $\mathbb{N}$. Next we want to show that the formula $\Gamma(a, n, m)$ gives a *good* definition of exponentiation also in $I\Delta_0 + \Omega_1$.

In any model of $I\Delta_0 + \Omega_1$ there is already a notion of exponentiation given by the Paris definition. So we will not attempt to prove the recursion laws for $\Gamma(x, y, z)$ directly, but instead we will show that $\Gamma(x, y, z)$ is equivalent to the Paris formula, $E_0(x, y, z)$ over $I\Delta_0 + \Omega_1$.

Theorem 5.1. $I\Delta_0 + \Omega_1 \vdash \forall x \forall y \forall z (E_0(x, y, z) \leftrightarrow \Gamma(x, y, z))$.

Proof. Let $\mathcal{M} \models I\Delta_0 + \Omega_1$ and $a, n, m \in \mathcal{M}$ satisfy $E(a, n, m)$. For convenience we will write a^n for m (there is no ambiguity since such an m is unique). Let $N = 2nm^2$ and consider the Pell equations $X^2 - (N^2a^2 - 1)Y^2 = 1$ and $X^2 - (N^2 - 1)Y^2 = 1$. First of all we have to guarantee the existence of $y_{n+1}(Na)$ and $y_{n+1}(N)$, since they have exponential size. By Remark 8(i), N^n is defined since it is of the order a^{n^2}, and by Lemma 2.4 we can deduce that both $y_{n+1}(Na)$ and $y_{n+1}(N)$ are defined. The proof that $a^n \leqslant y_{n+1}(Na)/y_{n+1}(N) < a^n + 1$ can be carried on in $\mathcal{M}$ exactly as done in $\mathbb{N}$, using the properties of summations proved in [3]. Notice that for any $N^* > N$ the inequalities are provable by a simple inspection of the proof done in $\mathbb{N}$.

Assume now that $a, n, m \in \mathscr{M}$ satisfy $m = [y_{n+1}(Na)/y_{n+1}(N)]$, where $N = 2nm^2$. From the existence of $y_{n+1}(Na)$ it follows that a^n is defined in the Paris sense, i.e. there is $s \in \mathscr{M}$ such that $E_0(a, n, s)$. We have to show that $m = s$. From the first part of this proof it follows that $s = [y_{n+1}(N^*a)/y_{n+1}(N^*)]$, where $N^* = 2ns^2$. If $s \leqslant m$ then $N^* \leqslant N$ and so $s \leqslant y_{n+1}(Na)/y_{n+1}(N) < s + 1$, which implies $s = m$. We want to exclude the case $m < s$. If so, $s \geqslant m + 1 > y_{n+1}(Na)/y_{n+1}(N)$, i.e. $sy_{n+1}(N) > y_{n+1}(Na)$. Recall that $s = a^n$, so

$$a^n \sum_{\substack{k \leqslant n+1 \\ k \equiv 1(2)}} \binom{n+1}{k} + N^{n+1-k}(N^2 - 1)^{(k-1)/2}$$

$$\geqslant \sum_{\substack{k \leqslant n+1 \\ k \equiv 1(2)}} \binom{n+1}{k} (Na)^{n+1-k}(N^2a^2 - 1)^{(k-1)/2}$$

and since N is a positive integer this is a contradiction. □

Corollary 5.2. $I\Delta_0 + \Omega_1 \vdash$

(i) $\forall x \forall y \forall z \forall w(\Gamma(x, y, z) \wedge \Gamma(x, y, w) \rightarrow z = w)$;

(ii) $\forall x \forall y \forall z(\Gamma(x, y, z) \rightarrow \Gamma(x, y + 1, xz))$;

(iii) $\forall x \forall y \forall z(\Gamma(x, y + 1, z) \rightarrow \exists w < z(\Gamma(x, y, w) \wedge z = xw))$.

We now give another definition of exponentiation in the language $\mathscr{L}^{\#}$ using only existentially bounded quantifiers, but this time we will prove all the recursion laws of the exponential function using induction only on $E_1^{\#}$-formulas, and a few axioms about $\#$.

We will work in the theory, denoted by $IE_1^{\#}$, which is axiomatized by:

(i) basic axioms for $+$ and $\cdot$;

(ii) induction scheme applied only to existentially bounded formulas of $\mathscr{L}^{\#}$;

(iii) axioms on $\#$:

(1) $\forall x(\#(x, 0) = 1 \wedge \#(x, 1) = 1)$,

(2) $\forall x \forall y > 0(\#(x, 2y) = x\#(x, y))$,

(3) $\forall x \forall y > 1(\#(x, y)/x = \#(x, y/2))$,

(4) $\forall x(\#(2, 2x) > x)$,

(5) $\forall x > 0(\#(2x, x) \leqslant x\#(x, x))$,

(6) $\forall x \forall y > 0 \forall z > 0(\#(x, yz) \geqslant \#(x, y)\#(x, z))$,

(7) $\forall x \forall y \leqslant x(\#(2x, y) < \#(2x - 1, 2y))$,

(8) $\forall x \forall y \forall z(\#(2, z) < y + 1 < \#(2, z + 1) \rightarrow \#(x, y + 1) = \#(x, y))$,

(9) $\forall x \forall y \forall z(\#(2, z) = y + 1 \rightarrow \#(x, y + 1) = x\#(x, y))$,

(10) $\forall x \forall y \forall z(y \leqslant z \rightarrow \#(x, y) \leqslant \#(x, z))$,

(11) $\forall x \forall z \forall y(\#(xz, y) = \#(x, y)\#(z, y))$,

(12) $\forall x \forall y \forall z(\#(x, y) = \#(x, z) \rightarrow \forall w\#(w, y) = \#(w, z))$.

If we interpret $\#$ in the standard model then axioms (1)–(12) are easily proved to be true. The only one which may seem not so straightforward is axiom (7). So we prefer to give a heuristic explanation of it. Let $a \in \mathbb{N}$, we want to find which $b \in \mathbb{N}$ satisfy the inequality

(†) $\quad \#(2a-1, 2b) > \#(2a, b).$

Inequality (†) is equivalent to show that

$$\#(2a-1, 2b) > \#(2a, b) \text{ iff } (2a)^{\log b} < (2a-1)^{\log b + 1}$$

$$\text{iff } \log b \log(2a) < (\log b + 1)\log(2a-1)$$

$$\text{iff } \log b(\log(2a) - \log(2a-1)) < \log(2a-1)$$

$$\text{iff } \log b < [\log(2a-1)]/[\log(2a) - \log(2a-1)].$$

By the Intermediate Value Theorem there is $\xi \in [2a-1, 2a]$ such that

$$\frac{\log(2a-1)}{\log(2a) - \log(2a-1)} = \xi \log(2a-1) > (2a-1)\log(2a-1).$$

So if we choose $b \in \mathbb{N}$ such that $[\log b] < (2a-1)\log(2a-1)$ then a, b satisfy (†). It is enough that b satisfies $\log b + 1 < (2a-1)\log(2a-1)$, i.e. $2b < (2a-1)^{2a-1}$, so $b < (2a-1)^{2a-1}$ will work. For our purposes it will be enough that $b \leqslant a$.

This axiom will guarantee that the intervals $[\#(2a-1, b), \#(2a, b)]$ and $[\#(2a-1, 2b), \#(2a, 2b)]$ have empty intersection.

Note. The theory $IE_1^{\#}$ may seem constructed *ad hoc* to prove properties of $\#$. However, we have added only universal true statements, so $IE_1^{\#}$ is not stronger with respect to provably recursive functions on $\mathbb{N}$ than the theory with only the induction scheme on existentially bounded formulas of $\mathscr{L}^{\#}$.

Lemma 5.3. *Let $\mathscr{M} \models IE_1^{\#}$, $x, y \in \mathscr{M}$. Then one of the following is true:*

$$\#(x, y+1) = \#(x, y) \text{ or } \#(x, y+1) = \#(x, 2y).$$

Proof. If there is a $z \in \mathscr{M}$ such that $\#(2, z) = y + 1$ then axiom (9) implies

$$\#(x, y+1) = x\#(x, y) = \#(x, 2y).$$

If there is no such a z, consider the set $A = \{z \in \mathscr{M} : \#(2, z) > y + 1\}$.

Axiom (4) implies $2(y+1) \in A$, so $A \neq \emptyset$. Hence there is $z_0 = \min(A)$, i.e. $\#(2, z_0 - 1) \leqslant y + 1 < \#(2, z_0)$. But we are assuming that there is no z such that $\#(2, z) = y + 1$, so $\#(2, z_0 - 1) < y + 1 < \#(2, z_0)$. By axiom 8, $\#(x, y+1) = \#(x, y)$. $\square$

In order to obtain an $E_1^{\#}$-definition of the relation $a^n = m$ we proceed in four steps. From now on we will work in a model $\mathcal{M}$ of the theory $IE_1^{\#}$. Let $1 < a \in \mathcal{M}$; we will refer to the Pell equation $X^2 - (a^2 - 1)Y^2 = 1$ as (★).

We have to develop part of the theory of Pell equations in $IE_1^{\#}$. Notice that we cannot use the notion of nth solution as the nth power of the fundamental solution as done in $I\Delta_0$. It is not known if there are *good* notions of summation and of binomial coefficient using only existentially bounded quantifiers.

Note. We recall that only algebraic tools are needed to prove that if x, y is a solution of (★) then so are

$$(x, y)(a, 1) = (ax + (a^2 - 1)y, ay + x) \quad \text{(denoted by } (x_*, y_*))$$

$$(x, y)/(a, 1) = (xa - (a^2 - 1)y, ay - x)) \quad \text{(denoted by } (x', y')).$$

We will use the above notation in what follows. Next lemma says that between y and y_* there is no other solution of (★).

Lemma 5.4. $\mathcal{M} \models \forall u \forall v \forall x \forall y (x^2 - (a^2 - 1)y^2 = 1 \wedge u^2 - (a^2 - 1)v^2 = 1 \wedge v > y \rightarrow v \geqslant y_*)$.

Proof. Fix $x, y, u, v \in \mathcal{M}$ solutions of (★) and assume $y < v < ay + x = y_*$, and so necessarily $x < u < ax + (a^2 - 1)y$. Consider $(u, v)/(x, y) = (ux - (a^2 - 1)vy, xv - uy)$, it is still a solution and satisfies $1 < ux - (a^2 - 1)vy < a$ and $0 < xv - uy < 1$, but there is no such a solution. Notice that no use of induction is made. □

Step 1. We first define the notion of $|b| + 1$-solution of (★), where $b \in \mathcal{M}$. Of course the previous statement looks unprecise since we do not have a notion of length yet. We will just say which size the solution is. Define

$$R(a, b, y) \stackrel{\text{def}}{=} \exists x \leqslant ay (x^2 - (a^2 - 1)y^2 = 1 \wedge \#(2a - 1, b) \leqslant y \leqslant \#(2a, b)).$$

The relation R says that y is a solution of (★) and satisfies (2) of Lemma 4.1.

Claim 1. $\mathcal{M} \models \forall b \leqslant a \exists y \leqslant \#(2a, a) R(a, b, y)$.

Proof. By induction on b.

$b = 0$: $\#(a, 0) = 1$, for all a. Then $y = 1$, the minimum nontrivial solution, satisfies $R(a, 0, 1)$.

$b \rightarrow b + 1 \leqslant a$: If $\#(2a, b + 1) = \#(2a, b)$, then there is nothing to prove since y satisfying $R(a, b, y)$ will satisfy also $R(a, b + 1, y)$.

Assume $\#(a, b + 1) = \#(a, 2b)$, and $R(a, b, y)$ for some $y \in \mathcal{M}$. Let x be the coordinate corresponding to y. Consider the successor solution $y_* = ay + x$ and

$x_* = xa + (a^2 - 1)y$. It is left to show that $\#(2a - 1, b + 1) \leqslant y_* \leqslant \#(2a, b + 1)$. From the definition of y_* and axioms (1)–(12) there follows

$$y_* \leqslant ay + ay = 2ay \leqslant 2a\#(2a, b) = \#(2a, 2b) = \#(2a, b + 1)$$

and

$$y_* > ay + \sqrt{a^2 + 1}\, y = (a + \sqrt{2a - 1})y \geqslant (2a - 1)\#(2a - 1, b)$$
$$= \#(2a - 1, 2b) = \#(2a - 1, 2b). \quad \square$$

Corollary 5.5. *If* $\mathcal{M} \models R(a, b, y)$ *then* $\mathcal{M} \models R(a, 2b, y_*)$, *i.e. if* $y \in [\#(2a - 1, b), \#(2a, b)]$ *then* $y_* \in [\#(2a - 1, 2b), \#(2a, 2b)]$.

Claim 2. $\mathcal{M} \models \forall b \leqslant a \forall y_1 \forall y_2 (R(a, b, y_1) \wedge R(a, b, y_2) \rightarrow y_1 = y_2)$, i.e. *R is functional.*

Proof. Let $b \leqslant a, y_1, y_2 \in \mathcal{M}$ satisfy $R(a, b, y_1)$ and $R(a, b, y_2)$, hence both y_1 and y_2 are in $[\#(2a - 1, b), \#(2a, b)]$. W.l.o.g. $y_1 < y_2$. Let x_1, x_2 be the corresponding first coordinates of the solutions y_1, y_2, respectively. Recall that between y_1 and $y_* = x_1 + ay_1$ there is no other solution of $(\star)$, so necessarily $y_1 < y_* \leqslant y_2$. Hence $y_* \in [\#(2a - 1, b), \#(2a, b)]$. By Corollary 5.5, $y_* \in [\#(2a - 1, 2b), \#(2a, 2b)]$, so the intervals $[\#(2a - 1, b), \#(2a, b)]$ and $[\#(2a - 1, 2b), \#(2a, 2b)]$ have a non-empty intersection. Contradiction. $\square$

The next lemma says that any solution $y \leqslant \#(2a, a)$ is the $(|b| + 1)$st solution for some $b \leqslant a$.

Lemma 5.6. $\mathcal{M} \models \forall x \leqslant a\#(2a, a)\ \forall y \leqslant \#(2a, a)\ (x^2 - (a^2 - 1)y^2 = 1 \rightarrow \exists b \leqslant a\ R(a, b, y))$.

Proof. By axiom (7) the interval $[0, \#(2a, a)]$ is partitioned into disjoint subintervals with endpoints $\#(2a - 1, b)$ and $\#(2a, b)$ for $b \leqslant a$. Let y be a solution smaller than $\#(2a, a)$ There are two cases:

Case (i): $y \in [\#(2a - 1, b), \#(2a, b)]$ for some $b \leqslant a$. Then we have finished.

Case (ii): $y \in (\#(2a, b), \#(2a - 1, 2b))$ and $2b \leqslant a$. We will show that this case never happens. Assume instead that it is true. By Claim 1 there are $w, z \in \mathcal{M}$ such that $w^2 - (a^2 - 1)z^2 = 1$ and $\#(2a - 1, b) \leqslant z \leqslant \#(2a, b)$. Consider $z_* = az + w$. Lemma 5.4 implies $z_* \leqslant y$ and Corollary 5.5, implies $z_* \in [\#(2a - 1, 2b), \#(2a, 2b)]$. So $y \geqslant \#(2a - 1, 2b)$, but this is in contradiction with $y \in (\#(2a, b), \#(2a - 1, 2b))$. $\square$

Combining Claim 1 and Lemma 5.6, we can deduce that all the solutions of $(\star)$ which are below $\#(2a, a)$ are bijectively distributed into the intervals $[\#(2a - 1, b), \#(2a, b)]$ for $b \leqslant a$.

Corollary 5.7. $\mathcal{M} \models \forall b \leqslant a \forall x \forall y (x^2 - (a^2 - 1)y^2 = 1 \wedge \#(2a - 1, b) \leqslant y \leqslant \#(2a, b) \rightarrow R(a, b/2, ay - x)$.

Proof. Fix b, x, y such that $\mathcal{M} \models R(a, b, y)$. By Lemma 5.6 there is a $d \leqslant a$ such that $\#(2a - 1, d) \leqslant y' \leqslant \#(2a, d)$, where $y' = ay - x$. Since $y = y'_*$ by Corollary 5.5, $\#(2a - 1, 2d) \leqslant y \leqslant \#(2a, 2d)$. If $\#(2a - 1, b) \neq \#(2a - 1, 2d)$ and $b < 2d$, then $\#(2a - 1, 2d) > \#(2a - 1, b)$ and so $\#(2a - 1, 2d) \geqslant (2a - 1)\#(2a - 1, b) = \#(2a - 1, 2b)$. But this give a contradiction since $y \leqslant \#(2a, b) < \#(2a - 1, 2b) \leqslant \#(2a - 1, 2d)$ and $y \geqslant \#(2a - 1, 2d)$.

If $2d < b$ then $\#(2a - 1, b) > \#(2a - 1, 2d)$, so $\#(2a - 1, b) \geqslant (2a - 1)\#(2a - 1, 2d) = \#(2a - 1, 4d)$. This implies $y \geqslant \#(2a - 1, 4d)$ which is in contradiction with $y \leqslant \#(2a, 2d) < \#(2a - 1, 4d)$. So the intervals $[\#(2a - 1, 2d), \#(2a, 2d)]$ and $[\#(2a - 1, b), \#(2a, b)]$ must coincide, i.e. $\#(2a - 1, 2d) = \#(2a - 1, b)$ and $\#(2a, 2d) = \#(2a, b)$. So

$$\#(2a - 1, d) = \frac{\#(2a - 1, 2d)}{2a - 1} = \frac{\#(2a - 1, b)}{2a - 1} = \#(2a - 1, b/2)$$

and

$$\#(2a, d) = \frac{\#(2a, 2d)}{2a} = \frac{\#(2a, b)}{2a} = \#(2a, b/2).$$

Hence $\mathcal{M} \models R(a, b/2, ay - x)$. □

Notation. We will write $y = y_{|b|+1}(a)$, $b \leqslant a$ to denote the unique y in $\mathcal{M}$ such that $\mathcal{M} \models R(a, b, y)$.

Step 2. We now introduce the notion of nth solution of (★).

Let $\theta(a, n, y) \stackrel{\text{def}}{=} \exists x \leqslant ay(x^2 - (a^2 - 1)y^2 = 1 \wedge y \equiv n (\text{mod}\, a - 1) \wedge y < \#(2a, a))$.

Notice that contrary to R, θ does not define a total relation for all $n \leqslant a - 2$: if $y \equiv a - 2 (\text{mod}\, a - 1)$ then we know that y is of the order a^a, and so it cannot be less or equal that $\#(2a, a)$. Roughly speaking, θ is defined for all $n \leqslant \log a$.

Claim 3. $\mathcal{M} \models \forall n \leqslant a - 2 \forall y_1 \forall y_2 (\theta(a, n, y_1) \wedge \theta(a, n, y_2) \rightarrow y_1 = y_2)$.

For the proof we need

Lemma 5.8. $\mathcal{M} \models \forall n \leqslant a - 2 \forall y (\theta(a, n, y) \rightarrow y \geqslant \#(a, n))$.

Proof. Fix $n, y \in \mathcal{M}$ such that $\mathcal{M} \models \theta(a, n, y)$, and let $\psi(k, y) \stackrel{\text{def}}{=} \exists z \leqslant y(\theta(a, k, z) \wedge z \geqslant \#(a, k))$. We prove by induction on k that $\mathcal{M} \models \forall k \leqslant n \psi(k, y)$.

$k = 0$: $z = 1$ works.

$k \to k+1 \leqslant n$: Let $z \leqslant y$ such that $\mathcal{M} \models \theta(a, k, z) \wedge z \geqslant \#(a, k)$, and let w be the corresponding first coordinate. Consider w_* and z_*; they are solution of (★) and $z_* \equiv k+1 (\mathrm{mod}\, a-1)$ (we have used Lemma 4.6). Moreover, $z_* > az + \sqrt{a^2-1}z = (a+\sqrt{a^2-1})z \geqslant a\#(a,k) \geqslant \#(a, k+1)$. □

Proof of Claim 3. The idea of the proof is to show that the bound $\#(2a, a)$ identifies the minimum solution of (★) in class n, and this will immediately imply functionality of θ.

Fix $n \leqslant a-2$ and y such that $\mathcal{M} \models \theta(a, n, y)$, and assume y is not minimum in class n; so there is a solution (x_1, y_1) of (★) such that $y_1 < y$ and $y_1 \equiv n (\mathrm{mod}\, a-1)$. Let

$$(x_0, y_0) = \frac{(x, y)}{(x_1, y_1)} = (xx_1 - (a^2-1)yy_1, x_1 y - xy_1).$$

(x_0, y_0) is a solution of (★), $y_0 \neq 0$ since $(x, y) < (x_1, y_1)$ and $y_0 \equiv 0 (\mathrm{mod}\, a-1)$. The solution

$$\frac{(x_0, y_0)}{(a, 1)} = (x_0', y_0')$$

satisfies $y_0' \equiv a-2 (\mathrm{mod}\, a-1)$. Lemma 4.5 implies that there is a solution in each class $m \leqslant a-2$. Let (u, v) be the minimum solution in class $a-2$. By Lemma 5.8, $v \geqslant \#(a, a-2)$. Then $v_* = av + u$ is the minimum nontrivial solution in class 0, and $v_* > (a+\sqrt{a^2-1})v \geqslant (a+\sqrt{a^2-1})\#(a, a-2) \geqslant a\#(a, a-2) \geqslant \#(a, a-1)$. Putting together all the inequalities we have got, it follows that $y = x_0 y_1 + x_1 y_0 > \sqrt{a^2-1}y_0 y_1 + \sqrt{a^2-1}y_0 y_1 = 2\sqrt{a^2-1}y_0 y_1 \geqslant 2\sqrt{a^2-1}v_* y_1 > 2\sqrt{a^2-1}\#(a, a-1)\#(a, n) > a\#(a, a-1)\#(a, n) = \#(a, 2(a-1))\#(a, n)$. But $\#(a, 2(a-1)) \geqslant \#(a, a)$ and $\#(a, n) \geqslant a$ for $n \geqslant 2$. So $y > \#(a, a)a \geqslant \#(2a, a)$ if $n \geqslant 2$. In case $n = 0, 1$ then $y = 0$ and $y = 1$ are the minimum solutions in class 0 and 1, respectively, and are smaller than $\#(2a, a)$. So $y > \#(2a, a)$ which is in contradict tion with $y < \#(2a, a)$. □

Remark 9. The formula θ gives an $E_1^{\#}$-definition of the relation $y = y_n(a)$, for small n. Unfortunately, θ does not define a total function since n has to be logarithmic with respect to a. But this is enough for our goals. The bound $\#(2a, a)$ identifies then the smallest solution in class n.

Notation. we will use $y = y_n(a)$ to denote the unique y, when it exists, such that $\mathcal{M} \models \theta(a, n, y)$.

Lemma 5.9. *Let* $a \geqslant c \in \mathcal{M}$. Then $\mathcal{M} \models \forall b \leqslant c \forall y_1 \leqslant \#(2a, a) \forall y_2 \leqslant \#(2c, c) \forall n < c-1 (R(a, b, y_1) \wedge R(c, b, y_2) \wedge y_2 \equiv n (\mathrm{mod}\, c-1) \to y_1 \equiv n (\mathrm{mod}\, a-1))$.

Proof. Fix $a, c \in \mathcal{M}$ and apply U_1-induction on b.

$b = 0$: $\#(2c-1,0) = \#(2c,0) = \#(2a-1,0) = \#(2a,0) = 1$. So $y_1 = y_2 = 1$ satisfy the property.

$b \to b+1 \leqslant c$: If $\#(2a,b+1) = \#(2a,b)$, hence by axiom (12), $\#(2a-1,b+1) = \#(2a-1,b)$, $\#(2c-1,b+1) = \#(2c-1,b)$ and $\#(2c,b+1) = \#(2c,b)$. In this case there is nothing to prove since it follows from the inductive hypothesis.

If $\#(2a,b+1) = \#(2a,2b)$, hence by axiom (12), $\#(2a-1,b+1) = \#(2a-1,2b)$, $\#(2c-1,b+1) = \#(2c-1,2b)$ and $\#(2c,b+1) = \#(2c,2b)$. Let $n, y_1, y_2 \in \mathcal{M}$ satisfy $\mathcal{M} \models R(a,b+1,y_1) \wedge R(c,b+1,y_2) \wedge y_2 \equiv n (\mathrm{mod}\, c-1)$, which is equivalent to $\mathcal{M} \models R(a,2b,y_1) \wedge R(c,2b,y_2) \wedge y_2 \equiv n (\mathrm{mod}\, c-1)$. Consider the solutions $(x_1', y_1') = (x_1, y_1)/(a,1)$ and $(x_2', y_2') = (x_2, y_2)/(c,1)$. Then $\mathcal{M} \models R(a,b,y_1') \wedge R(c,b,y_2') \wedge y_2' \equiv n-1 (\mathrm{mod}\, c-1)$, i.e. $\mathcal{M} \models R(a,b,y_1') \wedge R(c,b,y_2') \wedge y_2' \equiv n-1 (\mathrm{mod}\, c-1)$. So by inductive hypothesis $y_1' \equiv n-1 (\mathrm{mod}\, a-1)$, which implies $y_1 \equiv n (\mathrm{mod}\, a-1)$ (notice that we have used also Lemma 4.6). □

Step 3. We are now in a position to define the notion of length. Let $\lambda(b,n) \overset{\mathrm{def}}{=} \exists y \leqslant \#(2b,b)(R(b,b,y) \wedge \theta(b,n,y)) \vee (b = 1 \wedge n = 0) \vee (b = 0 \wedge n = 0)$.

The formula λ says that there is a solution y of $X^2 - (b^2-1)Y^2 = 1$ which is at the same time the nth solution and the $|b|+1$ solution, i.e. $y = y_n(b)$ and $y = y_{|b|+1}(b)$.

We need to prove some basic facts about λ.

Claim 4. *λ is functional, i.e.* $\mathcal{M} \models \forall b \forall n \forall m(\lambda(b,n) \wedge \lambda(b,m) \to n = m)$.

Proof. Fix $n, m, b \in \mathcal{M}$ such that both $\lambda(b,n)$ and $\lambda(b,m)$ are true in $\mathcal{M}$. Let y, z be the solutions of $X^2 - (b^2-1)Y^2 = 1$ satisfying $y \equiv n (\mathrm{mod}\, b-1)$, $z \equiv m (\mathrm{mod}\, b-1)$, and $y, z \in [\#(2b-1,b), \#(2b,b)]$; wlog $y < z$. This implies that the solution next to y, say y_*, satisfies $y < y_* \leqslant z$ and so $y_* \in [\#(2b-1,b), \#(2b,b)]$. But this is in contradiction with Corollary 5.5, so necessarily $y = z$, which implies $n = m$. □

Note. The notion of length should be thought in basis 2. We will use the notation $|b| = n$ for $\lambda(b,n)$.

Next we want to show that any element has a length.

Claim 5. $\mathcal{M} \models \forall b \exists n < b \lambda(b,n)$.

Proof. Fix $b \in \mathcal{M}$. By Claim 1 there is a y satisfying $R(b,b,n)$, which implies $y \leqslant \#(2b,b)$. Let $n < b-1$ be such that $y \equiv n (\mathrm{mod}\, b-1)$. The bound on y implies y is minimum in class n, so $y = y_n(b)$, hence $|b| = n$. □

Lemma 5.10. $\mathcal{M} \models \forall b \forall n < b(\lambda(b,n) \to \lambda(2b, n+1))$.

Proof. Fix $b \in \mathcal{M}$. By Claim 5 $\mathcal{M} \models \lambda(b,n) \wedge \lambda(2b,m)$ for some $n < b$ and $m < 2b$. We have to show $m = n+1$. Let y, z be such that $y = y_n(b)$ and $y = y_{|b|+1}(b)$, $z = y_m(2b)$

and $z = y_{|2b|+1}(2b)$. By Claim 1 there is a v such that $v = y_{|b|+1}(2b)$. Let u be the coordinate corresponding to v. By Lemma 5.9, $v \equiv n (\mathrm{mod}\, 2b - 1)$. Let $v_* = 2bv + u$, it satisfies $v_* \equiv n + 1 (\mathrm{mod}\, 2b - 1)$ and $R(2b, 2b, v_*)$. But $R(2b, 2b, z)$, so $z = v_*$, which implies $z \equiv n + 1 (\mathrm{mod}\, 2b - 1)$. Hence $m = n + 1$. □

Lemma 5.11. $\mathcal{M} \models \forall c \forall b \forall d \forall n < \min(b, d)(\lambda(b, n) \wedge \lambda(d, n) \rightarrow \#(c, b) = \#(c, d))$.

Proof. Fix $n, b, d \in \mathcal{M}$ such that $|b| = |d| = n$, and let y, z satisfy

$$y = y_n(b) = y_{|b|+1}(b) \quad \text{and} \quad z = y_n(d) = y_{|d|+1}(d).$$

W.l.o.g. $b \leqslant d$. By Claim 1 there is a v such that $v = y_{|b|+1}(d)$, and by Lemma 5.9, $v \equiv n (\mathrm{mod}\, d - 1)$. So in class n modulo $d - 1$ there are two solutions $z, v \leqslant \#(2d, d)$, hence necessarily $z = v$. But this implies $\#(2d, d) = \#(2d, b)$, so by axiom (12), $\#(c, d) = \#(c, b)$ for any c in $\mathcal{M}$. □

Step 4. We are now in a position to define exponentiation via the formula

$$\eta(a, n, m) \stackrel{\mathrm{def}}{=} \exists b < m(\lambda(b, n) \wedge \#(a, b) = m).$$

Since we work in $IE_1^{\#}$ we want to show that $\eta(a, n, m)$ defines a *good* notion of exponentiation, i.e. we will prove that η satisfies all the recursion properties of exponentiation in any model of $IE_1^{\#}$. The proofs of these properties are very simple at this point since they are heavily based on the theory of length we have developed until now in $IE_1^{\#}$.

Theorem 5.12. $IE_1^{\#} \vdash$

(1) $\forall x > 0 \eta(x, 0, 1)$;

(2) $\forall x \forall y \forall z \forall z_1(\eta(x, y, z) \wedge \eta(x, y, z_1) \rightarrow z = z_1)$;

(3) $\forall x \forall y \forall z(\eta(x, y, z) \rightarrow \eta(x, y + 1, zx))$;

(4) $\forall x \forall y \forall z(\eta(x, y + 1, z) \rightarrow \exists z_1 < z(\eta(x, y, z) \wedge z = z_1 x))$.

Proof. (1) Let $\mathcal{M} \models IE_1^{\#}$ and fix $a \in \mathcal{M}, a > 1$. From the definition of λ it follows $\lambda(1, 0)$ and so $\#(a, 1) = 1$.

(2) Let $a, n, m, m_1 \in \mathcal{M}$ satisfy $\mathcal{M} \models \exists b < m(\lambda(b, n) \wedge \#(a, b) = m)$ and $\mathcal{M} \models \exists d < m_1$ $(\lambda(d, n) \wedge \#(a, d) = m_1)$.

By Lemma 5.11, $\mathcal{M} \models \#(a, b) = \#(a, d)$, so $m = m_1$.

(3) Assume $\mathcal{M} \models \exists b < m(\lambda(b, n) \wedge \#(a, b) = m)$ for some a, m. By Lemma 5.10, $|2b| = n + 1$, and $\#(a, 2b) = a\#(a, b) = am$. The only thing left to show is $2b < am$, but this is clear since $2 \leqslant a$.

(4) Let $a, m \in \mathcal{M}$ such that $\mathcal{M} \models \exists b < m(|b| = n + 1 \wedge \#(a, b) = m)$. Consider $d = b/2$. By Claim 5 there is a t such that $|d| = t$, and by Lemma 5.10, $|2d| = |b| = t + 1$, so

necessarily $t = n - 1$. Moreover, $\#(a, d) = \#(a, b/2) = \#(a, b)/a = m/a$. So if $m_1 = m/a$ then $\eta(a, n, m_1)$ and $m_1 a = m$. □

6. Are $\binom{n}{k}$ and $n!$ $E_0^{\#}$-definable?

In this final section we consider other two functions, binomial coefficient and factorial. J. Robinson [13] gives an existential definition of the graphs of the above functions. Working on her definitions we try to bound the existential quantifiers, using terms in the language $\mathscr{L}^{\#}$. This would be the next natural step towards the proof of MRDP theorem in $I\Delta_0 + \Omega_1$. Unfortunately, we have not succeded in finding uniform $E_1^{\#}$-definitions of $\binom{n}{k} = m$ and $k! = m$. But we have some partial results.

We recall Robinson definitions

(†) $\binom{n}{k} = m$ iff m = remainder of division of $[(u+1)^n/u^k]$ by u, for $u > n^k$, and
(††) $k! = m$ iff $[n^k/\binom{n}{k}]$, where $n > (2k)^{k+1}$.

Clearly, functions of exponential growth are involved.

Consider first the binomial coefficient, and in particular the case of $\binom{2n}{n}$. Let $\binom{2n}{n} = m$. Recall that in $\mathbb{N}$ the following relation holds:

(★) $\quad 2^n \leqslant \binom{2n}{n} < 2^{2n}$.

A local version of it was proved for $I\Delta_0$ in [3]. Relation (★) implies that for any a, $a^n \leqslant \#(a, 2^n) \leqslant \#(a, m)$. Since we work in $\mathbb{N}$, there is no problem of existence of exponentials, so we need just to put the right bounds. In Robinson's definition we can choose any u such that $(2n)^n < u \leqslant 2^{n^2} \leqslant (\#(m, m))^2$.

Next step is to bound the size of $(u+1)^{2n}$. The following inequalities are true:

$$(u+1)^{2n} \leqslant (2u)^{2n} \leqslant 2^{2n}u^{2n} < m^2(\#(u, m))^2 \leqslant m^2(\#(\#(m, m)^2, m))^2$$

$$= m^2(\#(\#(m, m), m)\#(\#(m, m), m))^2 = m^2(\#(\#(m, m), m))^4.$$

The same bound works also for u^n. The notions of exponentiation, remainder and integer part are all $E_1^{\#}$-definable.

The above definition of $\binom{2n}{n} = m$ can be carried on in $I\Delta_0 + \Omega_1$. The relation (★) guarantees that 2^n is defined and so the same procedure works. Notice that if 2^n is defined in $\mathscr{M} \models I\Delta_0 + \Omega_1$ then 2^{n^k} are defined for all $k \in \mathbb{N}$, and also n^n is defined. This follows from the fact that we can define $2^{n^2} = \#(2^n, 2^n)$, $2^{n^3} = \#(\#(2^n, 2^n), 2^n)$, ... and $n^n = \#(n, 2^n)$.

We now examine the general case of $\binom{n}{k}$. W.l.o.g. we can assume $k \leqslant [n/2]$, since if $k > [n/2]$ then $\binom{n}{k} = \binom{n}{k - [n/2]}$. The following relation holds

(●) $\quad \binom{n}{i} \leqslant \binom{n}{k}$ for all $i \leqslant k \leqslant [n/2]$.

We first show how to reduce the size of u in (†). Consider the expression

$$\frac{(u+1)^n}{u^k} = \sum_{i=0}^{k-1} \binom{n}{i} u^{i-k} + \binom{n}{k} + \sum_{i=k+1}^{n} \binom{n}{i} u^{i-k}.$$

We want $\sum_{i \leqslant k-1} \binom{n}{i} u^{i-k} < 1$. It is enough if $\binom{n}{i} u^{i-k} < 1/k$ for all $i \leqslant k-1$. By (●), it is enough that $\binom{n}{k} u^{-1} < 1/k$, i.e. $u > mk$. The problems are still unsolved in bounding the size of u^n. Relation (★) is not true anymore, so we cannot bound an exponential in n in terms of $\binom{n}{k}$, since $\binom{n}{k}$ can be too small.

We now consider the relation $k! = m$, defined as in (††). Even if we assume to have an $E_1^{\#}$-definition of $\binom{n}{k}$, we still have problems in bounding the size of it in (††). From $2^k \leqslant k! = m$ it follows that $k^k \leqslant \#(k, m)$. So in (††) we can choose any n such that $\#(2k, m^2) < n \leqslant \#(m, m^2)$, and n^k can be bounded by $\#(n, m^2)$. Two problems are left: the definition of $\binom{n}{k}$ and its size. For what concerns the size we know that $\binom{n}{k} < 2^{2k^{2k}}$ and we cannot express double exponential in terms of $\#$. If we expand the language $\mathscr{L}^{\#}$ by adding another functional symbol which corresponds, roughly speaking, to $x^{\log x^{\log \log x}}$ (see also [16]), then we can easily bound the size of $\binom{n}{k}$, but there will be still left open the problem of defining $\binom{n}{k}$.

We can approach the problem of the definition of $k! = m$ in a different way using $\binom{2k}{k}$. Recall that

$$\binom{2k}{k} = \frac{(2k)!}{(k!)^2} = \frac{(k+1)(k+2)\cdots(2k)}{k!}.$$

So we can define

$$k! = m \text{ iff } m\binom{2k}{k} = (k+1)(k+2)\cdots(2k).$$

For what concerns the sizes of the elements involved in the above definition the following inequalities are true

$$\binom{2k}{k} < 2^{2k} < m^2 \quad \text{and} \quad (k+1)(k+2)\cdots(2k) \leqslant \#(m, m).$$

But unfortunately also this relation does not solve all the problems, since there is not an $E_1^{\#}$-formula, which is known to me, defining $(k+1)(k+2)\cdots(2k)$.

Acknowledgements

This paper is part of the author's D.Phil. thesis at Oxford University. He would like to thank Angus Macintyre for all his help during the preparation of the thesis.

References

[1] A. Baker, A Coincise Introduction to the Theory of Numbers, (Cambridge Univ. Press, Cambridge 1984).

[2] S. Buss, Bounded Arithmetic (Bibliopolis, Naples, 1986).
[3] P. D'Aquino, Local behaviour of the Chebyshev theorem in models of $I\Delta_0$, J. Symbolic Logic 57(1) (1992).
[4] C. Dimitracopoulos, Matijasevic theorem and fragments of arithmetic, Ph.D. Thesis, Manchester Univ., Manchester, 1980.
[5] H. Gaifman and C. Dimitracopoulos, Fragments of Peano's Arithmetic and the MRDP theorem, in: Logic and Algorithmic, Monographie No. 30 de L'Enseignement Mathematique, Geneve (1982) 187–206.
[6] G.H. Hardy and E.M. Wright, An Introduction to the Theory of Numbers (Oxford Univ. Press, Oxford, 3rd edn., 1954)
[7] J.P. Jones and V. Matijasevic, Proof of recursive unsolvability of Hilbert's tenth problem, Amer. Math. Montly 98 (1991) 689–709.
[8] R. Kaye, Diophantine induction, Ann. Pure Appl. Logic 46 (1990) 1–40.
[9] R. Kaye, Models of Peano Arithmetic (Oxford Univ. Press, Oxford, 1991).
[10] Y.I. Manin, A Course in Mathematical Logic, Graduate Text in Mathematics, Vol. 53 (Springer, Berlin, 1977).
[11] R. Parikh, Existence and feasibility in Arithmetic, J. Symbolic Logic 36 (1971) 494–508.
[12] J.B. Paris, A. Wilkie and A. Woods, Provability of the pigeonhole principle and the existence of infinitely many primes, J. Symbolic Logic 53 (1988) 1235–1244.
[13] J. Robinson, Existential definability in arithmetic, Trans. Amer. Math. Soc. 72 (1952) 437–449.
[14] J. Shepherdson, A non standard model for a free variable fragment of number theory, Bulletin de l'Academique Polonaise des Sciences, Série des Sciences, Mathematiques, Astronomique at Physiques 12 (1964) 79–86.
[15] A.J. Wilkie, Applications of complexity theory to Σ_0-definability problems in arithmetic, in: Pacholski et al., eds., Model Theory, Algebra and Arithmetic. Proc. Karpacz, Poland 1979. Lecture Notes in Mathematics, Vol. 834 (Springer, Berlin, 1980) 363–369. .
[16] A. Wilkie and J.B. Paris, On the scheme of induction for bounded arithmetic formulas, Ann. Pure Appl. Logic 35 (1987) 261–302.
[17] G. Wilmers, Bounded existential induction, J. Symbolic Logic 50 (1985) 72–90.
[18] A. Woods, Some problems in logic and number theory and their connections, Ph.D. Thesis, Univ. of Manchester, Manchester, 1981.